Cohomological Invariants of Quadratic Forms

Author: Ebony Ann Harvey

Boston College

The Graduate School of Arts and Sciences

Department of Mathematics

COHOMOLOGICAL INVARIANTS OF QUADRATIC FORMS

a thesis

by

EBONY ANN HARVEY

submitted in partial fulfillment of the requirements

for the degree of

Master of Arts

May 2010

ABSTRACT

Given a field F, an algebraic closure K and an F-vector space V, we can tensor the space V with the algebraic closure K. Two quadratic spaces of the same dimension become isomorphic when tensored with an algebraic closure. The failure of this isomorphism over F is measured by the Hasse invariant. This paper explains how the determinants and Hasse invariants of quadratic forms are related to certain cohomology classes constructed from specific short exact sequences. In particular, the Hasse invariant is defined as an element of the Brauer group.

Acknowledgements

I am very grateful for the opportunity to engage in research in order to continue to grow as a mathematician. Thank you Benjamin Howard for your willingness to serve as my advisor, for the guidance you facilitated, and for the support and assistance that you provided. Such a broad scope of research could not have been completed without your contribution. I would also like to thank Robert Meyerhoff and Solomon Friedberg for your consistent support throughout my tenure here and for helping me to fashion my time in the department such that I was able to reach maximal potential. To my mentor Mark Reeder, who has been a reservoir of inspiration and encouragement, never allowing me to make any excuses, and keeping me focused on the work at hand. To Avner Ash, for serving on the committee and offering valuable feedback during the revision process. Thanks to Jonathan Pottharst for the conversations and encouragement. A special thanks goes to the Boston College Mathematics Department for their assistance and support of this research, without which this journey would have been impossible. I am grateful for the time spent with all these individuals and I am indebted to them. I only hope that in my mathematical future I am able to repay them by pouring time, energy and faith into others as they have poured into me. Last but not least, to my family and friends who uniquely support me and champion my success, your love is invaluable and I am grateful.

Dedicated to

God the Father, God the Son

and

God the Holy Spirit

as first fruit of the harvest

Table of Contents

CHAPTER 1

Background Material

This chapter is a review of concepts, definitions, and theorems needed to understand the material in Chapter 2 and Chapter 3. We will study quadratic forms over a field of characteristic not equal to 2. If F is a field then $F^\times$ is the multiplicative group of units, $(F^\times)^2$ is the subgroup of squares and an element of the quotient of the quotient $F^\times/(F^\times)^2$ is called a square class. Throughout this paper let F be a field and ring mean ring with 1.

1. Quadratic Forms

1.1. Definitions of Quadratic Forms. A *quadratic form* $Q(x)$ in n variables over a field F is a homogenous polynomial of degree 2 with the coefficients $a_{ij} \in F$,

$$Q(x) = \sum_{i=1}^{n} a_{ii}x_i^2 + \sum_{i<j} a_{ij}x_ix_j.$$

A *symmetric bilinear form* on an F-vector space V is a map $\langle \cdot\,, \cdot \rangle \colon V \times V \to F$ satisfying

1. $\langle x + x', y\rangle = \langle x, y\rangle + \langle x', y\rangle$
2. $\langle ax, y\rangle = a\langle x, y\rangle$
3. $\langle x, y\rangle = \langle y, x\rangle$

for all $x, x', y \in V$ and $a \in F$.

Given a finite dimensional F-vector space V a quadratic form is a function $Q\colon V \to F$ satisfying $Q(ax) = a^2Q(x)$, for all $a \in F, x \in V$ and making the function

$$2\langle x, y\rangle_Q \mapsto Q(x+y) - Q(x) - Q(y)$$

a symmetric bilinear form. Choose a basis of V, say $\{e_1, \ldots, e_n\}$ and let $\langle e_i, e_j\rangle_Q = a_{ij}$. Let $A \in M_n(F)$ be the matrix whose entry in the i^{th}-column and j^{th}-row is the coefficient a_{ij} of $Q(x)$. The matrix $A = (a_{ij})$ is called the *matrix associated to* $Q(x)$. A is symmetric and we can write the quadratic form as $Q(x) = x^t \cdot A \cdot x$, $x \in V$. The pair (V, Q), sometimes written (V, A) is called a *quadratic space*. The dimension of (V, Q) is the dimension of the underlying vector space V. The terms quadratic space and quadratic form may be used interchangeably. A quadratic space (V, Q) is called *isotropic* if there exists $x \in V$ such that $Q(x) = 0$. We say Q *represents* 0. The space is called *anisotropic* if Q does not represent 0.

1.2. Translations of Quadratic Forms. Suppose Q_1 and Q_2 have rank n and m over F respectively. Addition is defined by $Q_1 \perp Q_2 = Q_1(x_1, \ldots, x_n) + Q_2(x_{n+1}, \ldots, x_{n+m})$. Subtraction is defined by $Q_1 \perp (-Q_2)$. A vector x is *orthogonal* to a vector y if $\langle x, y\rangle = 0$. A vector space V is the direct sum of two subspaces $V = V_1 \oplus V_2$, if $V = V_1 + V_2, V_1 \cap V_2 = \{0\}$ and $\langle v_1, v_2\rangle = 0$ for all $v_1 \in V_1, v_2 \in V_2$. For quadratic spaces (V_1, Q_1) and (V_2, Q_2) the space

$$(V_1, Q_1) \oplus (V_2, Q_2) = (V_1 \oplus V_2, Q_1 \perp Q_2)$$

is called the *orthogonal sum*. The matrix associated to (V, Q) is

$$A = \begin{bmatrix} A_1 & 0 \\ 0 & A_2 \end{bmatrix}$$

where A_i is the matrix associated to V_i. Two quadratic spaces $(V_1, Q_1), (V_2, Q_2)$ are *isometric* if there is an isomorphism $\phi\colon V_1 \to V_2$ such that $Q_2(\phi(x)) = Q_1(x)$ for all $x \in V_1$.

Definition 1.1. Two quadratic forms Q_1 and Q_2 of dimension n are *equivalent*, $Q_1 \sim Q_2$, if either of the two equivalent statements hold

1. The quadratic spaces $(F^n, Q_1) \cong (F^n, Q_2)$ are isometric.
2. There exists $P \in \mathrm{GL}_n(F)$ such that $A_2 = P^t A_1 P$ where A_i is the matrix of Q_i.

This definition implies that P is the *change of basis* matrix from linear algebra and the equivalence of quadratic forms corresponds to a change of basis of the quadratic spaces. The determinants of A_1 and A_2 differ by a square because $\det A_2 = (\det P)^2 \det A_1$. Usually we call any representative in the square class the determinant. A quadratic form is called *degenerate* if $\det A = 0$ and *nondegenerate* otherwise.

Theorem 1.1. *Every quadratic space V has an orthogonal basis.*

Proof. If V has dimension 1 the statement is automatic, therefore suppose that V has dimension $n > 1$ and assume that the theorem holds for spaces of dimension up to $n - 1$. If for any $v \in V$ $\langle v, v\rangle_Q = 0$ then any basis is orthogonal, so we can assume

that there exists a vector $v_1 \in V$ such that $\langle v_1, v_1 \rangle_Q \neq 0$. Let V_1 be the 1-dimensional subspace spanned by v_1 and decompose V as the direct sum of $V = V_1 \oplus W$ where W is the orthogonal complement of V_1. W has an orthogonal basis, $u_2, \ldots, u_n$ by assumption and $v_1, u_2, \ldots u_n$ is an orthogonal basis for V [**6**]. □

Corollary 1.2. *Let Q be a quadratic form in n variables. Then there exists constants $a_1, \ldots, a_n \in F$ such that $Q \sim a_1 x_1^2 + \cdots + a_n x_n^2$.*

This tells us that for any quadratic form the associated matrix A can be diagonalized, which is to say an orthogonal basis defines an isometry $(V, Q) \cong (F^n, Q')$ where $Q'(x_1, \ldots, x_n) = a_1 x_1^2 + \cdots + a_n x_n^2$ with $Q(e_i) = a_i \in F$. If every element of F is a square we can scale each a_i to 0 or 1. The *rank* of Q is equal to the number of indices i such that $a_i \neq 0$ and the *discriminant* is the number $d(Q) = a_1 a_2 \cdots a_n = \det A$. A form is nondegenerate if and only if the rank is n or equivalently $d(Q) \neq 0$.

1.3. The Hilbert Symbol. In this section let F denote either the field of real numbers $\mathbb{R}$ or the field of p-adic numbers $\mathbb{Q}_p$, $p \in \mathbb{N}$ a prime number.

Definition 1.2. Let $a, b \in F^\times$. Write

$$(a, b) = \begin{cases} 1 & \text{if } ax^2 + by^2 = z \text{ has a non zero solution } (x, y, z) \in F^3 \\ -1 & \text{otherwise} \end{cases}$$

The number (a, b) is called the *Hilbert Symbol* of a and b relative to F.

The Hilbert symbol is symmetric and bilinear.

1.4. Quadratic Forms over $\mathbb{Q}_p$. In this section all quadratic spaces (and quadratic forms) over $\mathbb{Q}_p$ are nondegenerate.

Definition 1.3. Let (V, Q) be a quadratic space of rank n with discriminant $d(Q)$. For all $a_i \in \mathbb{Q}_p^\times$ define the *Hasse invariant* as

$$\epsilon(\mathfrak{e}) = \prod_{i<j}(a_i, a_j) = \pm 1$$

where $\mathfrak{e} = e_1, \ldots, e_n$ is an orthogonal basis of V and $(\ ,\ )$ is the Hilbert symbol.

Theorem 1.3. *The Hasse invariant is an invariant, i.e. it does not depend on the choice of the orthogonal basis.*

Before we prove this theorem we need to prove a theorem about the relationship between different orthogonal bases.

Theorem 1.4 (Witt's Chain Equivalence)**.** *Let (V, Q) be a non-degenerate quadratic space. If $\mathcal{B} = \{e_1, \ldots, e_n\}$ and $\mathcal{B}' = \{e'_1, \ldots, e'_n\}$ are both orthogonal bases of V, then there exists a chain of orthogonal bases $\mathcal{B}_0, \mathcal{B}_1, \ldots, \mathcal{B}_m$ with $\mathcal{B}_0 = \mathcal{B}$ and $\mathcal{B}_m = \mathcal{B}'$ such that $\mathcal{B}_{j-1}$ and $\mathcal{B}_j$ are contiguous (i.e. they differ by at most 2 vectors) for $0 \leq j \leq m$.*

Proof. There is nothing to prove for dimension $n = 1, 2$ so we will assume V has dimension $n \geq 3$ and apply induction. Write e'_1 as a linear combination of $\mathcal{B}$ and let $k = k(\mathcal{B})$ be the number of nonzero coefficients in the representation,

$$e'_1 = \sum_{j=1}^{k} a_j e_j$$

where $a_j \neq 0$ $(1 \leq j \leq k)$. If $k = 1$ we can replace e_1 by e'_1 and write $\mathcal{B}_1 = \{e'_1, e_2, \ldots, e_n\}$. Apply the induction hypothesis to the subspace of vectors orthogonal

to e_1' and we get the theorem. Now suppose $k \geq 2$. Then

$$0 \neq (e_1', e_1') = a_1^2(e_1, e_1) + \cdots + a_k^2(e_k, e_k)$$

with each term on the right nonzero. Without loss of generality suppose $a_1^2(e_1, e_1) + a_2^2(e_2, e_2) \neq 0$. We can assume this because if the sum of the first two terms is zero then $k > 2$ and either the sum of the first and third terms is nonzero or the sum of the second and third term is nonzero. Let $f_1 = a_1e_1 + a_2e_2$, $f_2 = e_1 + be_2$, $f_j = e_j$ $(3 \leq j \leq n)$ where $b = -a_1(e_1, e_1)/a_2(e_2, e_2)$. Then $\mathcal{B}_1 = \{f_1, \ldots, f_n\}$ is an orthogonal basis and

$$e_1' = f_1 + \sum_{j=3}^{k} a_j f_k.$$

Therefore $k(\mathcal{B}_1) < k(\mathcal{B})$. Replace $\mathcal{B}$ by $\mathcal{B}_1$ and repeat the procedure until after m steps we get an orthogonal basis with $k(\mathcal{B}_m) = 1$. Then we can apply the induction hypothesis as above. □

Proof of Theorem 1.3. Now we prove the invariance of the Hasse invariant, following [7]. If $n = 1$, $\epsilon(\mathfrak{e}) = 1$. If $n = 2$, $\epsilon(\mathfrak{e}) = 1$ if and only if $a_1x^2 + a_2y^2 = z^2$ has a non trivial solution. For $a_1x^2 + a_2y^2 = z^2$ to have a non trivial solution $a_1x^2 + a_2y^2$ must represent 1 which means there exists a $v \in V$ such that $Q(v) = 1$ and this does not depend on $\mathfrak{e}$. For $n \geq 3$ we use induction. Let $\mathfrak{e}'$ be another orthogonal basis of V. By Witt's Chain Equivalence, there is a chain of orthogonal basis which are pairwise contiguous so without loss of generality let $\mathfrak{e}$ and $\mathfrak{e}'$ be contiguous. The Hilbert symbol is symmetric so we may permute the basis elements in $\mathfrak{e}'$ to assume

$e_1' = e_1$. If $a_i' = e_i' e_i'$, then $a_1' = a_1$ and

$$\epsilon(\mathfrak{e}) = (a_1, a_2 \cdots a_n) \prod_{2 \le i < j} (a_i, a_j)$$

$$= (a_1, a_1 d(Q)) \prod_{2 \le i < j} (a_i, a_j)$$

$$\epsilon(\mathfrak{e}') = (a_1, a_1 d(Q)) \prod_{2 \le i < j} (a_i', a_j').$$

Then

$$\prod_{2 \le i < j} (a_i, a_j) = \prod_{2 \le i < j} (a_i', a_j')$$

by the inductive hypothesis applied to the orthogonal complement of e_1 as in step 1 above. □

Theorem 1.5. *Quadratic spaces over $\mathbb{Q}_p$ are in one-to-one correspondence with triples (n, d, ϵ) where n is the rank of Q, $d = d(Q)$ and $\epsilon = \epsilon(Q)$ is the Hasse invariant of Q under the restrictions that $\epsilon = 1$ if $n = 1$ or $(n, d) = (2, -1)$.*

Proof. Showing two equivalent quadratic forms have the same rank, discriminant and Hasse invariant follows from the above definitions. To prove the converse we use induction on the rank n of two forms. Let $a, b \in \mathbb{Q}_p^\times$. Suppose that $n = 2$ and let $Q = a(x_1^2 + dx_2^2)$ and $Q' = b(y_1^2 + dy_2^2)$ with $(a, ad) = (b, bd)$. Then $(-d, a) = (-d, b)$ thus $(-d, ab) = 1$. Then $x_1^2 + dx_2^2$ represents ab so Q represents b and since the discriminants are equal modulo squares Q is equivalent to Q'. Now let Q and Q' have rank n and suppose the theorem is true for quadratic forms of rank $n - 1$. By Theorem 6 and its corollary in [**6**] both Q and Q' represent all elements of $\mathbb{Q}_p^\times / (\mathbb{Q}_p^\times)^2$

so there exists $a \in \mathbb{Q}_p^\times$ represented at the same time by Q and Q' allowing us to write $Q \sim aX^2 + q$ and $Q' \sim aX^2 + q'$ where q, q' are quadratic forms of rank $n-1$. The forms q and q' have the same invariants and by hypothesis $q \sim q'$. Calculating invariants we see the relations

$$d(q) = ad(Q) = ad(Q') = d(q')$$

$$\epsilon(q) = \epsilon(Q)(a, d(q)) = \epsilon(Q')(a, d(Q')) = \epsilon(q').$$

hence $Q \sim Q'$. □

1.5. Quadratic Forms over $\mathbb{Q}$. Let all quadratic forms be nondegenerate and let V be the set of prime numbers together with the symbol ∞ with $\mathbb{Q}_\infty = \mathbb{R}$. We have the following invariants,

1. The discriminant $d(Q) \in \mathbb{Q}^\times/(\mathbb{Q}^\times)^2$
2. View Q as a quadratic form over $\mathbb{Q}_v$, denoted Q_v via the injection $\mathbb{Q} \to \mathbb{Q}_v$, for $v \in V$. The invariants of Q_v are
   (a) $d_v(Q)$ which is the image of $d(Q)$ by $\mathbb{Q}^\times/(\mathbb{Q}^\times)^2 \to \mathbb{Q}_v^\times/(\mathbb{Q}_v^\times)^2$;
   (b) $\epsilon_v(Q)$ defined by

$$\epsilon_v(Q) = \prod_{i<j} (a_i, a_j)_v. \tag{1}$$

3. The quotient $\mathbb{R}^\times/(\mathbb{R}^\times)^2$ has two elements $\{\pm 1\}$ therefore with respect to an orthogonal basis the diagonal entries of the associated matrix A_Q can be chosen as 1 or -1. Let r be the number of 1's and s the number of -1's. The *signature* (r, s) of the real quadratic form Q_∞ is uniquely determined.

Hilbert's product formula gives the relationship $\prod_{v\in V}\epsilon_v(Q)=1$;

1.6. The Orthogonal Group. We denote the group of isometries of the quadratic space (V,Q) by $\mathcal{O}_Q$. This group consists of all matrices T such that $T^tMT=M$ for the matrix $M=\big(\langle e_i,e_j\rangle_Q\big)$. These T are called *automorphs* of M and this relationship tells us that $\mathcal{O}_Q\subset \mathrm{GL}_n(F)$ and if $T\in\mathcal{O}_Q$ then $\det T=\pm 1$.

2. Galois Groups

Let F be a field and define $\mathrm{Aut}(F)$ to be the group of all automorphisms of F. If K/F is a field extension then $\mathrm{Aut}(K/F)\subset\mathrm{Aut}(K)$ is the subgroup of automorphisms of K which restrict to the identity on F. If $H\subset\mathrm{Aut}(K)$ is a subgroup we define the *fixed field* of H as

$$K^H=\{\alpha\in K\mid \sigma\alpha=\alpha,\ \forall\sigma\in H\}.$$

For any finite extension K/F, $|\mathrm{Aut}(K/F)|\le[K:F]$ with equality if K/F is normal and separable. When we have $|\mathrm{Aut}(K/F)|=[K:F]$, K is said to be *Galois* over F, K/F is a *Galois extension* and the group of automorphisms $\mathrm{Aut}(K/F)$ is called the *Galois group* of K/F, denoted $\mathrm{Gal}(K/F)$. If $\alpha\in K$ the elements $\sigma\alpha$ for $\sigma\in\mathrm{Gal}(K/F)$ are called the *conjugates* of α over F.

Theorem 2.1 (The Fundamental Theorem of Galois Theory)**.** *Let K/F be a Galois extension and set $G=Gal(K/F)$. There is a bijection*

$$\{L\colon F\subset L\subset K\}\longleftrightarrow\{H\colon H<G\}$$

given by the correspondence

$$\begin{aligned} L &\longmapsto \{\sigma \in G \colon \forall \alpha \in L \ \sigma\alpha = \alpha\} \\ H &\longmapsto L^H \end{aligned}$$

which are inverses of each other. This bijection is called the Galois correspondence and satisfies

(1) *(inclusion reversing)* $L^{H_1} \subset L^{H_2}$ *if and only if* $H_2 \subset H_1$

(2) $[K : L] = |H|$ *and* $[L : F] = |G : H|$

(3) K/L *is always Galois with Galois group* $Gal(K/L) = H$

(4) L *is Galois over* F *if and only if* H *is a normal subgroup in* G.

3. Clifford Algebras

3.1. Tensor Product, Extension of Scalars. Given a quadratic space (V, Q) we want to be able to extend scalars from F to K where K/F is a field extension. We state the necessary tools to do this here.

Claim. Let $f : R \to S$ a ring homomorphism with $1_R \mapsto 1_S$. Then $S \otimes_R R \simeq S$ as left S-modules.

Proof. Consider the map $\varphi \colon S \times R \to S$ given by $(s, r) \mapsto sf(r) = sr$. This map is R-balanced

$$\varphi(s_1 + s_2, r) = (s_1 + s_2)r = s_1 r + s_2 r = \varphi(s_1, r) + \varphi(s_2, r)$$

$$\varphi(sr, r') = (sr)r' = s(rr') = \varphi(s, rr').$$

By the universal property for tensor products we have an associated group homomorphism $\Phi\colon S \otimes_R R \to S$ defined by $\Phi(s \otimes r) = sr$. Φ is an S-module homomorphism

$$\Phi(s'(s \otimes r)) = \Phi(s's \otimes r) = s'sr = s'\Phi(s \otimes r).$$

The inverse to Φ is $\Phi^{-1}\colon S \to S \otimes_R R$ defined by $s \mapsto s \otimes 1$ □

Theorem 3.1. *[Tensor Product of Direct Sums] Let M, M' be right R-modules and let N, N' be left R-modules. Then there are unique group isomorphisms*

$$(M \oplus M') \otimes_R N \simeq (M \otimes_R N) \oplus (M' \otimes_R N)$$

$$M \otimes_R (N \oplus N') \simeq (M \otimes_R N) \oplus (M \otimes_R N')$$

such that $(m, m') \otimes n \mapsto (m \otimes n, m' \otimes n)$ and $(m \otimes (n, n') \mapsto (m \otimes n, m \otimes n')$ respectively.

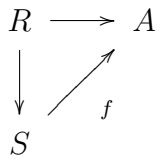
This theorem extends by induction to any finite direct sum of R-modules [**1**].

Corollary 3.2. *The module obtained from the free R-module $N \simeq R^n$ by extension of scalars from R to S is the free S-module S^n, i.e. $S \otimes_R R^n \simeq S^n$ as left S-modules.*

As mentioned above, consider the case when we have the field extension K/F and $V \simeq F^n$. Then $V \otimes_F K$ is a vector space over the larger field K of the same dimension (because from above we have $V \otimes_F K \simeq K^n$) and $V \subset V \otimes_F K$ as an F-vector subspace.

3.2. Central Simple Algebras. Given a commutative ring R with 1, an *R-algebra* S is a ring with 1 together with a ring homomorphism $R \to S$ mapping $1_R \mapsto 1_S$ such that the image of R lies in center of S. The map is called the *structure*

map of the algebra S. If S is a commutative ring we call this a *commutative* R-algebra. The homomorphism need not be injective, for example $\mathbb{Z}/n\mathbb{Z}$ is a $\mathbb{Z}$-algebra via the usual map $\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$, but when $R = F$, F a field, the map $F \to S$ is injective. If S and A are R-algebras, a *homomorphism of R-algebras* is a ring homomorphism $f\colon S \to A$ taking $1_S \mapsto 1_A$ and making the diagram



commute where the unlabeled arrows are the structure maps. Let S be an F-algebra with center $Z(S)$. If $F = Z(S)$ we say that S is a *central* F-algebra. An algebra is called *simple* if it contains no nontrivial proper two sided ideals. We say S is *central simple* if S is both central and simple. If S and T are central simple F-algebras then so is $S \otimes_F T$ (See [**1**] for a proof).

Let R be a ring with 1. Call R° the *opposite ring* which has the same additive group but whose multiplication is defined by $r \cdot x = xr$. There is an isomorphism $End_R(R) \simeq R^\circ$ and using this we prove that if S is a finite central simple F-algebra then $S \otimes_F S^\circ \simeq M_n(F)$ where $n = [S : F]$.

Proposition 3.3. *$S \otimes S^\circ \simeq M_n(F)$ with $n = [S : F]$.*

Proof. (Following [**2**]) For all $s \in S$ define $L_s \in End_F(S)$ by $L_s(x) = sx$ and $R_s \in End_F(S)$ by $R_s(x) = xs$. Let $A = \{L_s\colon s \in S\}$ and $B = \{R_s\colon s \in S\}$. Then $A \simeq S$ and $B \simeq S^\circ$ as rings. Elements of A and B commute by associativity of S.

Define $S \otimes S^\circ \to End_F(S)$ by $s \otimes s' \mapsto L_s \circ R_{s'}$. Since S and S° are simple $S \otimes S^\circ$ is simple giving injectivity. Also $\dim_F(S \otimes S^\circ) = (\dim_F(S))^2 = \dim_F(\mathrm{End}_F(S))$ giving surjectivity. Since $M_n(F) \simeq End_F(S)$ we have the required isomorphism. □

Now we state the Skolem-Noether Theorem whose results will be needed in later proofs and classically is necessary for the Wedderburn and Frobenius Theorems. For a proof see page 93 of [**2**].

Theorem 3.4 (Skolem-Noether)**.** *Let S be a finite dimensional central simple F-algebra and let R be a simple F-algebra. If $f, g\colon R \to S$ are injective homomorphisms then there is an inner automorphism $\alpha\colon S \to S$ such that $\alpha f = g$.*

Equivalently, If R_1 and R_2 are isomorphic simple subalgebras of S, then for any isomorphism $f\colon R_1 \to R_2$ there is an inner automorphism α of S such that $\alpha|_{R_1} = f$. In particular, any automorphism of S is inner.

3.3. Graded Algebras.

Definition 3.1. A *graded* F-algebra is an F-algebra C together with a decomposition $C = C_0 \oplus C_1$ of C as an F-vector space such that

1. $F \subset C_0$
2. $C_iC_j \subset C_{i+j},\ i, j \in \{0, 1\}$ with $i + j \in \mathbb{Z}/2\mathbb{Z}$

It may help to think of C as having an even part C_0 and an odd part C_1. A homomorphism of graded F-algebras is a homomorphism $\varphi\colon C \to D$ of algebras such that $\varphi(C_i) \subset D_i$. If $C = C_0 \oplus C_1$ and $D = D_0 \oplus D_1$ are two graded F algebras the *graded tensor product* of C and D, $C\hat{\otimes}D$ is the usual tensor product $C \otimes_F D$ as a

vector space but with

$$(C\hat{\otimes}D)_0 = (C_0 \otimes D_0) \oplus (C_1 \otimes D_1)$$

$$(C\hat{\otimes}D)_1 = (C_0 \otimes D_1) \oplus (C_1 \otimes D_0)$$

$$(c_i \otimes d_j)(c'_k \otimes d'_l) = (-1)^{jk}(c_i c'_k \otimes d_j d'_l)$$

with $c_i \in C_i, d_j \in D_j$. The maps

$$i_C \colon C \to C\hat{\otimes}D, \quad c \mapsto c \otimes 1$$

$$i_D \colon D \to C\hat{\otimes}D, \quad d \mapsto 1 \otimes d$$

have the universal property that for any homomorphism of graded F-algebras $\varphi \colon C \to T, \vartheta \colon D \to T$ whose images anticommute $\varphi(c_i)\vartheta(d_j) = (-1)^{ij}\vartheta(d_j)\varphi(c_i)$ there is a unique homomorphism $\psi \colon C\hat{\otimes}D \to T$ such that $\varphi = \psi \circ i_C$ and $\vartheta = \psi \circ i_D$.

Definition 3.2. Let $c_1, \ldots, c_n \in F$ and define $C(c_1, \ldots, c_n)$ to be the F-algebra with generators $f_1, \ldots, f_n$ and the relationships $f_i^2 = c_i$, $f_i f_j = -f_j f_i$ $(i \neq j)$. A basis for $C(c_1, \ldots, c_n)$ as an F-vector space is the set

$$\mathcal{B} = \{f_1^{i_1} \cdots f_n^{i_n} \colon i_j \in \{0, 1\}\}$$

$$\text{where} \quad C_0 = \{f_1^{i_1} \cdots f_n^{i_n} \colon i_1 + \cdots + i_n \text{ even}\}$$

$$\text{and} \quad C_1 = \{f_1^{i_1} \cdots f_n^{i_n} \colon i_1 + \cdots + i_n \text{ odd}\}$$

3.4. The Clifford Algebra. Let V be an F-vector space and (V, Q) a quadratic space.

Definition 3.3. The *Clifford Algebra* $C(V,Q)$ is the quotient of the tensor algebra

$$T(V) = \bigoplus_{n\geq 0} V^{\otimes n} = V \oplus (V \otimes V) \oplus (V \otimes V \otimes V) \oplus \cdots$$

of V by the two sided ideal $I(Q)$ generated by the elements $x \otimes x - Q(x)$.

Let $\rho\colon V \to C(V,Q)$ be the composite of the canonical map $V \to T(V)$ with the quotient map $T(V) \to C(V,Q)$. For all $x \in V$, $\rho(x)^2 = Q(x) \cdot 1_C$ ($C = C(V,Q)$) and if x is anisotropic then $\rho(x)$ is invertible with inverse $\rho(x)/Q(x)$. For any F-algebra A and any F-linear map $\varphi : V \to A$ with $\varphi(x)^2 = Q(x) \cdot 1_A$, there exists a unique F-algebra homomorphism $\varphi'\colon C \to A$ such that the diagram

$$\begin{array}{ccc} V & \xrightarrow{\varphi} & A \\ {\scriptstyle\rho}\downarrow & \nearrow_{\varphi'} & \\ C & & \end{array}$$

commutes. This describes a universal property for the Clifford algebra [**3**], so we may say the pair $\big(C(V,Q),\rho\big)$ is unique up to isomorphism. Another consequence of the universal property is that any isometry $\phi\colon (V_1,Q_1) \to (V_2,Q_2)$ induces an isomorphism $C(\phi)\colon \big(C(V_1,Q_1),\rho\big) \to \big(C(V_2,Q_2),\rho\big)$ [**3**]. From now on we will identify $F \cdot 1_C$ with F.

By linearity, $\rho(x+y)^2 = \big(\rho(x)+\rho(y)\big)^2 = \rho(x)^2 + \rho(x)\rho(y) + \rho(y)\rho(x) + \rho(y)^2$ and $\rho(x+y)^2 = Q(x+y) = Q(x) + Q(y) + 2\langle x,y\rangle$, thus $\rho(x)\rho(y) + \rho(y)\rho(x) = 2\langle x,y\rangle_Q$. Let $e_1,\ldots,e_n$ be an orthogonal basis for V. We have $\rho(e_i)^2 = Q(e_i)$ and $\rho(e_i)\rho(e_j) = -\rho(e_j)(e_i)$ $(i \neq j)$. If we let $Q(e_i) = c_i$ there is a surjective homomorphism $e_i \mapsto \rho(e_i)$ from $C(c_i,\ldots,c_n)$ onto $C(V,Q)$; in fact, we will see this is an F-algebra isomorphism.

The Clifford algebra is a graded F-algebra. We can decompose $T(V)$ into an even or odd part in the following way: $T(V)$ is spanned by products of even, respectively odd, numbers of vectors so we write

$$T(V) = T(V)_0 \oplus T(V)_1$$

$$T(V)_0 = \bigoplus_{m \text{ even}} V^{\otimes m}$$

$$T(V)_1 = \bigoplus_{m \text{ odd}} V^{\otimes m}.$$

In particular, $T(V)$ is graded by degree. The generators $x \otimes x - Q(x)$ of $I(Q)$ have even degree so we may decompose the ideal as

$$I(Q) = \big(I(Q) \cap T(V)_0\big) \oplus \big(I(Q) \cap T(V)_1\big)$$

so that

$$C(V,Q) = C_0 \oplus C_1$$

with $C_i = T(V)_i / I(Q) \cap T(V)_i$ [**4**].

Theorem 3.5. *Let (V,Q) be a quadratic space of dimension n.*

(1) *For every orthogonal basis for (V,Q) the homomorphism $C(c_1,\ldots,c_n) \to C(V,Q)$ via the map $f_i \mapsto \rho(e_i)$ is an isomorphism.*

(2) *For every orthogonal decomposition $(V,Q) = (V_1,Q_1) \oplus (V_2,Q_2)$ the homomorphism $C(V,Q) \to C(V_1,Q_1)\hat{\otimes}C(V_2,Q_2)$ is an isomorphism.*

(3) *The dimension of $C(V,Q)$ as an F-vector space is 2^n.*

PROOF. Suppose $n = 1$. The space V has basis e and $Q(e) = \langle e, e\rangle = c$. $T(V)$ is a polynomial algebra in one indeterminate e, $T(V) = F[e], I(1) = \langle e^2 - c\rangle$ so $C(V,Q) \simeq C(c)$. (2) and (3) are clear. Assume the theorem is true for $\dim(V) < n$. We can decompose $(V,Q) = (V_1,Q_1) \oplus (V_2,Q_2)$ such that $\dim(V_i) < n$. The homomorphism

$$C(V,Q) \longrightarrow C(V_1,Q_1)\hat{\otimes}C(V_2,Q_2)$$

defined by

$$x = (x_1,x_2) \mapsto \rho(x_1)\otimes 1 + 1\otimes\rho(x_2)$$

is surjective because the image contains the simple tensors $\rho(x_1)\otimes 1, \rho(x_2)\otimes 1$ which generate $C(V_1,Q_1)\hat{\otimes}C(V_2,Q_2)$. So

$$\dim(C(V,Q)) \geq 2^{\dim V_1}2^{\dim V_2} = 2^n.$$

Since we can always find an orthogonal basis for (V,Q) we get

$$C(V,Q) \to C(V_1,Q_1)\hat{\otimes}\cdots\hat{\otimes}C(V_n,Q_n)$$

which means that $\dim(C(V,Q)) \leq 2^n$ therefore $\dim(C(V,Q)) = 2^n$ and the homomorphisms are isomorphism [**3**][**4**]. □

Corollary 3.6. *The map $\rho\colon V \longrightarrow C(V,Q)$ is injective; therefore, consider $V \subset C(V,Q)$.*

By this corollary we will omit writing the map ρ and identify V with its image $\rho(V) \subset C(V,Q)$.

3.5. The Center of the Clifford Algebra. Let (V, Q) be nondegenerate of dimension $n > 0$, $e_1, \ldots, e_n$ be an orthogonal basis for (V, Q), $Q(e_i) = c_i$ and $A = (\langle e_i, e_j \rangle)$ the associated matrix. Theorem 3.5 showed that we have an isomorphism $C(c_1, \ldots, c_n) \to C(V, Q)$. In $C(c_1, \ldots, c_n)$

$$(e_1 \cdots e_n)^2 = (-1)^{\frac{n(n-1)}{2}} c_1 \cdots c_n = (-1)^{\frac{n(n-1)}{2}} \det(A) = \Lambda.$$

Additionally,

$$e_i \cdot (e_1 \cdots e_n) = (-1)^{i-1} c_i (e_1 \ldots e_{i-1} e_{i+1} \ldots e_n)$$

$$(e_1 \cdots e_n) \cdot e_i = (-1)^{n-i} c_i (e_1 \ldots e_{i-1} e_{i+1} \ldots e_n);$$

therefore, $e_i \ldots e_n \in Z(C)$ if and only if n is odd.

Theorem 3.7. *Let (V, Q) be nondegenerate of dimension $n > 0$ over F.*

(1) *For n even, $Z(C) = F$.*

(2) *For n odd, $Z(C)$ is degree 2 over F and generated by the element $e_1 \cdots e_n$ with $(e_1 \cdots e_n)^2 = \Lambda$.*

See [**3**] for a proof. We will concern ourselves with n even because then $C(V, Q)$ is a central simple F-algebra. For $a, b \in F^\times$ let $\left(\frac{a, b}{F}\right)$ denote the F-algebra of dimension 4 with the basis $1, i, j, k$ satisfying the relations $i^2 = a, j^2 = b, ij = -ji = k$. This is called the *generalized quaternion algebra*. If $c_1, c_2 \in F^\times$ $C(c_1, c_2)$ is isomorphic to the generalized quaternion algebra $\left(\frac{c_1, c_2}{F}\right)$. One can show that every 4-dimensional central simple algebra over F is isomorphic to $\left(\frac{a, b}{F}\right)$ for some $a, b \in F^\times$.

3.6. The Clifford Group, Γ. Let γ be an F-algebra automorphism of $C(V,Q)$ defined by

$$\gamma(t) = \begin{cases} t & \text{if } t \in C_0(V,Q) \\ -t & \text{if } t \in C_1(V,Q) \end{cases}.$$

Definition 3.4. The *Clifford Group* is

$$\Gamma_Q(F) = \{t \in C(V,Q) \colon t \,\text{invertible},\ \gamma(t)Vt^{-1} = V\}.$$

For $t \in \Gamma_Q(F)$ let $\alpha(t) : V \longrightarrow V$ be the homomorphism defined by

$$\alpha(t) \colon x \mapsto \gamma(t)xt^{-1}. \tag{2}$$

Proposition 3.8. *For all $t \in \Gamma_Q(F)$, $\alpha(t)$ is an isometry of V and*

$$1 \longrightarrow F^\times \longrightarrow \Gamma_Q(F) \xrightarrow{\alpha} \mathcal{O}_Q(F) \longrightarrow 1$$

is exact.

Proof. [**4**] To show $\alpha(t)$ is an isometry first define an *involution* of the Clifford Algebra as an F-linear map $\star \colon C(V,Q) \to C(V,Q)$ by $a^\star = a$ for all $a \in V$ with the property $(ab)^\star = b^\star a^\star$. Given $t \in \Gamma_Q(F)$, by definition $\gamma(t)V = Vt$ and $\gamma(t^\star) = Vt^\star$. Thus, $t^\star \in \Gamma_Q(F)$. For all $x \in V$

$$\gamma(t)xt^{-1} = -\gamma\big(\gamma(t)xt^{-1}\big)^\star = -\gamma\big(t^{\star-1}x\gamma(t^\star)\big) = \gamma(t^{\star-1})xt^\star$$

which implies $\gamma(t^\star)\gamma(t)x = xt^\star t$. Since $Q(x) = x^\star x$ for all $x \in V$, we have

$$Q\big(\alpha(t)(x)\big) = \alpha(t)(x)^\star \cdot \alpha(t)(x) = t^{\star-1}x\gamma(t^\star)\cdot\gamma(t)xt^{-1} = t^{\star-1}xxtt^\star tt^{-1} = t^{\star-1}x^2t^\star$$

$$= t^{\star-1}Q(x)t^\star = Q(x).$$

To show that this sequence is exact we need the kernel of α to be $F^\times$ and α to be surjective. As $F \in Z(\Gamma_Q(F))$, $F^\times \subset \ker(\alpha)$. For the converse let $t_0 \in C_0(V,Q)$, $t_1 \in C_1(V,Q)$ and $t = t_0 + t_1 \in \Gamma_Q$ such that $\gamma(t)xt^{-1} = x$ for all $x \in V$. This means $t_0x = xt_0$ and $t_1x = -xt_1$. Since V generates $C(V,Q)$ these equations imply that t_0 is in the center, and hence $t_0 \in F$. Thus t_1 centralizes C_0 so $t_1 = 0$ because it follows from Theorem 3.7 that no nonzero element of C_1 centralizes C_0. So $\ker(\alpha) = F^\times$. See [**4**] or [**8**] for surjectivity. □

4. The Brauer Group

4.1. The Brauer Group and the Relative Brauer Group. We want to define a notion of equivalence classes of finite dimensional simple central F-algebras. It can be shown that if D is a finite dimensional division algebra with center F the ring $M_n(D)$ is simple with center $Z(M_n(D)) = K \cdot I_n$ where I_n is the identity matrix. Conversely if S is a finite dimensional simple F-algebra there exists a finite dimensional division algebra D such that $A \simeq M_n(D)$. If D and E are finite dimensional division algebras such that $M_n(D) \simeq M_m(E)$ then $D \simeq E$ and $n = m$. This can be proven by showing the existence of an isomorphism $D^\circ \simeq End_{M_n(D)}(N)$ where N is

any simple $M_n(D)$-module. We have the following theorem by Wedderburn-Artin as a result (see pages 17-20 of [**3**] for proofs).

Theorem 4.1 (Wedderburn-Artin Structure Theorem)**.** *Let S be a finite dimensional simple F algebra. Then $S \simeq M_n(D)$ for a suitable division algebra D. The integer n is uniquely determined by S and D is determined up to an isomorphism.*

Now we define a notion of similarity for central simple F-algebras.

Definition 4.1. If S and T are finite-dimensional central simple F-algebras we say S and T are *similar*, writing $S \sim T$, if any one of the equivalent properties holds:

1. If $S \simeq M_n(D)$ and $T \simeq M_n(E)$ for division algebras D, E then $D \simeq E$.
2. There exist m, n such that $S \otimes_F M_m(F) \simeq T \otimes_F M_n(F)$.
3. There exist m, n such that $M_m(S) \simeq M_n(T)$.
4. If M is the unique simple S-module and N is the unique simple T-module then $\mathrm{End}_S(M) \simeq \mathrm{End}_T(N)$.

Such division algebras exist because of Theorem 4.1. We are trying to classify all finite-dimensional central simple F-algebras up to similarity. We will soon show the equivalence classes form a group using the next two lemmas.

Lemma 4.2. (1) *$M_n(A) \simeq A \otimes_F M_n(F)$ for any F-algebra A.*

(2) *$M_m(F) \otimes M_n(F) \simeq M_{mn}(F)$*

Proof. (1) Let $I \in M_n(A)$ be the identity matrix. We can map $A \to M_n(A)$ via the map $a \mapsto aI$ and we have the inclusion map $M_n(F) \to M_n(A)$. For all $X \in M_n(A), (aI)X = aX = Xa = X(aI)$ so we can map $f\colon A \otimes_F M_n(F) \to M_n(A)$

by $1 \otimes e_{ij} \mapsto e_{ij}$, where e_{ij} is the matrix with 1 in the ij-position. Conversely there is a $g\colon M_n(A) \to A \otimes_F M_n(F)$ with $e_{ij} \mapsto 1 \otimes e_{ij}$. The composition $f \circ g$ is the identity on $M_n(A)$ and $g \circ f$ is the identity on $A \otimes_F M_n(F)$. These maps are inverses of each other showing the isomorphism. (2) Let $A = M_m(F)$ above. Then $M_m(F) \otimes M_n(F) \simeq M_n(M_m(F)) \simeq M_{nm}(F)$ [**2**]. □

Lemma 4.3. *If $S \sim S_1$ and $T \sim T_1$ then $S \otimes T \sim S_1 \otimes T_1$.*

Proof. By the definition of similarity, S and S_1 have isomorphic division algebras and T and T_1 have isomorphic division algebras. Let D, respectively E, be the division algebra. So $S \simeq M_n(D), S_1 \simeq M_{n_1}(D), T \simeq M_m(E), T_1 \simeq M_{m_1}(E)$. Then

$$\begin{aligned} S \otimes T &\simeq M_n(D) \otimes M_m(E) \\ &\simeq D \otimes M_n(F) \otimes E \otimes M_m(F) \\ &\simeq D \otimes E \otimes M_{nm}(F) \\ &\simeq M_{nm}(D \otimes E) \end{aligned}$$

Similarly $S_1 \otimes T_1 \simeq M_{n_1 m_1}(D \otimes E)$ so by condition one of the definition of similar we have $S \otimes T \sim S_1 \otimes T_1$. [**2**] □

Lemma 4.2 shows that the operation of the tensor product is well-defined on similarity classes. Thus, we may multiply equivalence classes by multiplying any two representatives and then taking the equivalence class of the product.

Definition 4.2. The *Brauer group* of a field F, denoted $Br(F)$, is the set of equivalence classes of finite-dimensional central simple F-algebras under the equivalence

relation of similarity, with tensor product the group operation and the equivalence class of F acting as the identity element.

We will denote the equivalence class of a central simple algebra S in the Brauer group by $[S]$. The Brauer group is trivial if F is the only central F-algebra up to similarity. For all n, $[M_n(F)] = [F]$. It also follows that for S and T of the same dimension over F, $S \sim T$ if and only if $[S] = [T]$ in $Br(F)$.

Theorem 4.4. *The Brauer group $Br(F)$ with the operation $[S] \bullet [T] = [S \otimes T]$ is an abelian group.*

PROOF. First note that $S \otimes T$ is a finite-dimension central simple F-algebra. We showed above that the tensor product gives a well-defined multiplication. Associativity follows from associativity of the tensor product. The identity is $[F]$ because $F \otimes_F S \simeq S$. By Proposition 3.3 $[S^\circ]$ is the inverse of $[S]$. Abelian follows from the fact that $S \otimes T \simeq T \otimes S$. [**2**] □

If K/F is a field extension there is a homomorphism $Br(F) \to Br(K)$ defined by $[S] \mapsto [S_K]$ where $S_K = K \otimes_F S$ is the extension of scalars.

Definition 4.3. The *relative Brauer group*, denoted $Br(K/F)$, is the kernel of the above homomorphism, $\ker\big(Br(F) \to Br(K)\big)$.

The next proposition gives us a nice result on the dimension of simple central F-algebras [**2**].

Proposition 4.5. *If D is a finite dimensional division algebra with center F, then $[D : F]$ is a square.*

In general, given a finite dimensional simple central F-algebra S and a finite dimensional division algebra D with center F such that $S \simeq M_n(D)$ we have

$$[S : F] = [S : D][D : F] = n^2 \cdot [D : F] = n^2 \cdot m^2 = (nm)^2$$

for some $m \in \mathbb{N}$.

Definition 4.4. Let S be a simple F-algebra. A *maximal subfield* of S is a field K such that $F \subset K \subset S$ and K is its own centralizer in S.

Definition 4.5. Let D be a division algebra over F. A field K over F is called a *splitting field* for D if D, when considered over K, is isomorphic to $M_n(K)$. Then D_K splits as a sum of n simple K-modules, whereas D is simple as a module over itself.

In particular, if K is a separable maximal subfield of the F-algebra S and L is a splitting field for K relative to F, then L splits S. For example L could be an algebraic closure of F, or if K is Galois, we could take $L = K$.

Theorem 4.6. *Let S be a central simple F-algebra of dimension n^2. Then any maximal subfield K of S is a splitting field for S, and $[S : K] = [K : F] = n$. Conversely, given any field extension K/F of degree n, any element $[S] \in Br(K/F)$ has a unique representative S of degree n^2 which contains K as a maximal subfield.*

This theorem tells us that we can choose the representative S of the equivalence class $[S]$ which contains K as a maximal subfield and where K splits S. This theorem also implies that we can consider a division algebra D of degree n^2 over F and pick K to be a Galois extension of F which is a splitting field for D, and in this specific

case we are able to describe the elements of the Brauer group explicitly [**2**]. The next corollary tells us that we can reduce our study of $Br(F)$ to the study of $Br(K/F)$ to the case when K/F is Galois.

Corollary 4.7. *$Br(F) = \bigcup Br(K/F)$, where K ranges over the finite Galois extensions of F.*

4.2. Factor Sets.

Definition 4.6. Given a Galois extension K/F with Galois group G a *factor set* is a collection of elements $\{f_{\sigma,\tau} \in K^\times : \sigma, \tau \in G\}$ satisfying $\rho(f_{\sigma,\tau})f_{\rho,\sigma\tau} = f_{\rho,\sigma}f_{\rho\sigma,\tau}$ for all $\sigma, \tau, \rho \in G$.

Definition 4.7. We say two factor sets $\{f_{\sigma,\tau}\}$ and $\{g_{\sigma,\tau}\}$ are *related* and write $\{f_{\sigma,\tau}\} \sim \{g_{\sigma,\tau}\}$ if they satisfy the relation

$$g_{\sigma,\tau} = \frac{u_\sigma \sigma(u_\tau)}{u_{\sigma\tau}} f_{\sigma,\tau} \tag{$\dagger$}$$

for some collection of $\{u_\sigma \in K^\times : \sigma \in G\}$.

For the rest of this section let S be a central simple F-algebra of dimension n^2 containing K as a maximal subfield. Assume that K/F is Galois, let $[K : F] = n$ and $G = \mathrm{Gal}(K/F)$. By Skolem-Noether (Theorem 3.4) for any $\sigma \in G$ there exists $s_\sigma \in S^\times$ such that

$$s_\sigma a s_\sigma^{-1} = \sigma(a) \qquad \text{for all } a \in K.$$

Let $s'_\sigma \in S^\times$ such that $s'_\sigma a s'^{-1}_\sigma = \sigma(a)$ for all $a \in K$. Write $u_\sigma = s'_\sigma s_\sigma^{-1}$ and one can show that u_σ commutes with all elements in K, therefore $u_\sigma \in K^\times$. We would like to

know whether or not $s_\sigma s_\tau = s_{\sigma\tau}$. On the one hand,

$$\sigma\tau(a) = \sigma(\tau(a)) = s_\sigma \tau(a) s_\sigma^{-1} = s_\sigma s_\tau a s_\tau^{-1} s_\sigma^{-1},$$

but on the other hand,

$$\sigma\tau(a) = s_{\sigma\tau} a s_{\sigma\tau}^{-1}.$$

This gives $s_\sigma s_\tau a s_\tau^{-1} s_\sigma^{-1} = s_{\sigma\tau} a s_{\sigma\tau}^{-1}$ which we simplify to $s_\sigma s_\tau = f_{\sigma,\tau} s_{\sigma\tau}$ where $f_{\sigma,\tau} = s_\sigma s_\tau s_{\sigma\tau}^{-1} \in K^\times$ is a scalar. The set $\{f_{\sigma,\tau}\}$ is a factor set and we have shown that given a central simple F-algebra S with maximal subfield K, Galois over F, we can attach a factor set, which we will call the *factor set of S relative to K*. It will be useful to think of $\{s_\sigma\}$ as a function from $G \to K^\times$ and a factor set $\{f_{\sigma,\tau}\}$ as a function from $G \times G \to K^\times$.

Given S, once we fix K we may still construct different factor sets by different choices of $s_\sigma \in K^\times$, but the factor sets are related which we now show. Suppose $\{f_{\sigma,\tau}\}$ and $\{g_{\sigma,\tau}\}$ are factor sets of S relative to K defined by the elements $\{s_\sigma\}$ and $\{s'_\sigma\}$ respectively. As above there exists $u_\sigma \in K^\times$ such that $s'_\sigma = u_\sigma s_\sigma$. Then

$$s'_\sigma s'_\tau = u_\sigma s_\sigma u_\tau s_\tau$$

$$g_{\sigma,\tau} s'_{\sigma,\tau} = u_\sigma s_\sigma u_\tau (s_\sigma^{-1} s_\sigma) s_\tau$$

$$= u_\sigma \sigma(u_\tau) s_\sigma s_\tau$$

$$g_{\sigma,\tau} u_{\sigma\tau} s_{\sigma\tau} = u_\sigma \sigma(u_\tau) f_{\sigma,\tau} s_{\sigma\tau}$$

$$g_{\sigma,\tau} u_{\sigma\tau} = u_\sigma \sigma(u_\tau) f_{\sigma,\tau}.$$

The last line shows that $\{f_{\sigma,\tau}\}$ and $\{g_{\sigma,\tau}\}$ are related. We *normalize* a factor set by choosing $s_1 = 1$ and thus making $f_{1,\sigma} = f_{\sigma,1} = 1$ for all $\sigma \in G$.

Proposition 4.8. *The set $\{s_\sigma\}$ is a basis for S over K.*

PROOF. Because $|G| = [K : F] = [S : K]$ it suffices to show that the $\{s_\sigma\}$ are linearly independent. Suppose the set is not independent and choose a maximal subset J such that $J \subset G$ and the elements $\{s_\tau \colon \tau \in J\}$ are linearly independent. Assume $\sigma \notin J$. There is a set $\alpha_\tau \in K$ such that

$$s_\sigma = \sum_{\tau \in J} \alpha_\tau s_\tau.$$

Multiply both sides by $k \in K$

$$s_\sigma \cdot k = \sum_{\tau \in J} \alpha_\tau s_\tau \cdot k$$

to get the relation

$$\sigma(k) s_\sigma = \sum_{\tau \in J} \alpha_\tau \tau(k) s_\tau.$$

But also $\sigma(k)s_\sigma = \sum \alpha_\tau \sigma(k) s_\tau$ so

$$\sum_{\tau \in J} \alpha_\tau \tau(k) s_\tau = \sum_{\tau \in J} \alpha_\tau \sigma(k) s_\tau$$

which means $\alpha_\tau \tau(k) = \alpha_\tau \sigma(k)$ for all $\tau \in J$ and $k \in K$. By assumption $s_\sigma \neq 0$ thus there exists a $\tau \in J$ with $\alpha_\tau \neq 0$ such that $\tau(k) = \sigma(k)$. This means that $\sigma = \tau$ which is a contradiction to our choice of σ. Thus $J = G$ [**2**]. □

In general a function $\{f_{\sigma,\tau}\}\colon G\times G\to K^\times$ is not the factor set of a central simple algebra. By associativity we must have $s_\rho(s_\sigma s_\tau)=(s_\rho s_\sigma)s_\tau$ and this implies

$$s_\rho f_{\sigma,\tau}s_{\sigma\tau}=f_{\rho,\sigma}s_{\rho\sigma}s_\tau$$

$$s_\rho f_{\sigma,\tau}(s_\rho^{-1}s_\rho)s_{\sigma\tau}=f_{\rho,\sigma}s_{\rho\sigma}s_\tau$$

$$\rho(f_{\sigma,\tau})f_{\rho,\sigma\tau}s_{\rho\sigma\tau}=f_{\rho,\sigma}f_{\rho\sigma,\tau}s_{\rho\sigma\tau}$$

$$\rho(f_{\sigma,\tau})f_{\rho,\sigma\tau}=f_{\rho,\sigma}f_{\rho\sigma,\tau}\tag{‡}$$

which gives the necessary condition on $\{f_{\sigma,\tau}\}$ to make it a factor set.

Proposition 4.9. *Given a Galois extension K/F, any factor set $\{f_{\sigma,\tau}\}$ is the factor set relative to K of a central simple F-algebra S containing K as a maximal subfield. S is called the crossed product of K and G relative to the factor set $\{f_{\sigma,\tau}\}$ or the crossed product algebra and we write $S=(K,G,f)$.*

Proof. Let S be a vector space over K with basis $\{e_\sigma\colon \sigma\in G\}$. We will define multiplication by

$$(\alpha e_\sigma)(\beta e_\tau)=\alpha\sigma(\beta)f_{\sigma,\tau}e_{\sigma\tau}$$

and extend to S by linearity. We check that S is an algebra. The distributive property and compatibility with scalars follows from the definitions. Associativity follows

$$\begin{aligned}\big((\alpha e_\sigma)(\beta e_\tau)\big)(\gamma e_\rho)&=\big(\alpha\sigma(\beta)f_{\sigma,\tau}e_{\sigma\tau}\big)(\gamma e_\rho)\\&=\alpha\sigma(\beta)f_{\sigma,\tau}\sigma\tau(\gamma)f_{\sigma\tau,\rho}e_{\sigma\tau\rho}\\&=\alpha\sigma(\beta)\sigma\tau(\gamma)f_{\sigma,\tau}f_{\sigma\tau,\rho}e_{\sigma\tau\rho}\end{aligned}$$

$$= \alpha\sigma(\beta)\sigma\tau(\gamma)\sigma(f_{\tau,\rho})f_{\sigma,\tau\rho}e_{\sigma\tau\rho} \quad by\ (\ddagger)$$

$$= \alpha\sigma\big(\beta\tau(\gamma)f_{\tau,\rho}\big)f_{\sigma,\tau\rho}e_{\sigma\tau\rho}$$

$$= (\alpha e_\sigma)\big(\beta\tau(\gamma)f_{\tau,\rho}e_{\tau,\rho}\big)$$

$$= (\alpha e_\sigma)\big((\beta e_\tau)(\gamma e_\rho)\big).$$

For any $\sigma \in G$ we must have $1(f_{1,\sigma})f_{1,\sigma} = f_{1,1}f_{1,\sigma}$ by $(\ddagger)$, therefore $f_{1,1} = f_{1,\sigma}$ and

$$(f_{1,1}^{-1}e_1)e_\sigma = f_{1,1}^{-1}f_{1,\sigma}e_\sigma = f_{1,1}^{-1}f_{1,1}e_\sigma = e_\sigma.$$

But also $\sigma(f_{1,1}) = f_{\sigma,1}f_{\sigma,1}f_{\sigma,1}^{-1} = f_{\sigma,1}$ so

$$e_\sigma(f_{1,1}^{-1}e_1) = \sigma(f_{1,1}^{-1})f_{\sigma,1}e_\sigma = f_{\sigma,1}^{-1}f_{\sigma,1}e_\sigma = e_\sigma$$

showing that the identity element is $f_{1,1}^{-1}e_1$. The map $K \to S, a \mapsto a \cdot (f_{1,1}^{-1}e_1)$ shows that $K \subset S$ as a ring. What is $Z(K)$? First $\sum a_\sigma e_\sigma \in Z(K)$ if and only if

$$a\left(\sum a_\sigma e_\sigma\right) = \left(\sum a_\sigma e_\sigma\right)a$$

for all $a \in K$. Above we saw that $aa_\sigma = a_\sigma\sigma(a)$ and putting these together we see that if $a_\sigma \neq 0$ then $\sigma(a) = a$, i.e. $\sigma = 1$ so $Z(K) \subset K$. But $K \subset Z(K)$ so $Z(K) = K$ in S shows that S is central. To show that S is simple suppose that I is a nonzero proper two-sided ideal in S and let $\varphi\colon K \to S/I$. Since $\ker(\varphi)$ is trivial, φ is an injection and $Im(\varphi)$ is a subring of S/I. Let $\varphi(e_\sigma) = \bar{e}_\sigma$ and by the same argument we used above $\{\bar{e}_\sigma\}$ is a linearly independent set. Thus $\dim_K(S/I) = \dim_K(S)$ implies $I = 0$ so S is simple [**1**][**2**]. $\square$

Theorem 4.10. *Let K/F be a Galois extension with Galois group G. There is a bijective correspondence between elements of $Br(K/F)$ and equivalence classes of factor sets $\{f_{\sigma,\tau}\}$ relative to K, where two factor sets are equivalent if they are related in the sense defined above.*

PROOF. Given $x \in Br(K/F)$ by Theorem 4.6 there exists a central simple algebra S such that $[S] = x$, which contains K as a maximal subfield. Different choices of S will give related factor sets giving the map

$$Br(K/F) \longmapsto \text{equivalence classes of } \{f_{\sigma,\tau}\}$$

$$[S] \longmapsto (\text{factor set of } S \text{ relative to } K)$$

which is well-defined. Conversely given a factor set $\{f_{\sigma,\tau}\}$ there exists a central simple algebra (K, G, f) with that factor set. So we have the map

$$\text{equivalence classes of } \{f_{\sigma,\tau}\} \longmapsto Br(K/F)$$

$$\{f_{\sigma,\tau}\} \longmapsto [(K, G, f)]$$

which can be shown to be well-defined and which is an inverse to the map constructed above [**2**]. □

CHAPTER 2

Cohomology

1. Preliminaries

1.1. Non-commutative Cohomology. Let G be a group and A a nonempty set. Define a *left action* of G on A to be a function $\bullet\colon G\times A \to A$ written $(g,a)\mapsto g\bullet a$ such that for all $a\in A, 1_G \bullet a = a$ and for all $g_1, g_2 \in G, g_1 \bullet (g_2 \bullet a) = (g_1 g_2)\bullet a$. For simplicity we write $g\bullet a$ as ga. A is called a *G-set*. If A is a group and left action respects the group structure, $g(a_1a_2) = g(a_1)g(a_2)$ for all $a_1, a_2 \in A$, we call A a *G-group*.

Definition 1.1. Define the *zeroth cohomology set of G in A*, $H^0(G,A)$, as the set of elements of A fixed under G which we will notate by A^G

If A is a G-group, then $H^0(G,A)$ is a subgroup. Suppose A is a G-group. A map $G\to A$ denoted by $g\mapsto a_g$ is called a *1-cocycle* of G in A if it satisfies $a_{g_1g_2} = a_{g_1}(g_1 a_{g_2})$ for all $g_1, g_2 \in G$. Two 1-cocycles a_g and a'_g are called *equivalent* if there exists a $b\in A$ such that $a'_g = b^{-1}a_g(gb)$ for all $g\in G$. This is an equivalence relation on the set of 1-cocycles.

Definition 1.2. Define the *first cohomology set of G in A*, $H^1(G,A)$, to be the set of equivalence classes of 1-cocycles.

$H^1(G, A)$ is a pointed set with a distinguished element, the equivalence class of the constant 1-cocycle $a_g = 1_A$ [**7**].

Definition 1.3. A group homomorphism $f\colon A \to B$ is called a *G-homomorphism* if $f(ga) = g(f(a))$ for all $g \in G$ and $a \in A$.

If a_g is a 1-cocycle of G in A then $b_g = f(a_g)$ is a 1-cocycle of G in B [**4**]. The next section will show that if A and B are abelian, $H^i(G, A)$ and $H^i(G, B)$ for $i = 0, 1$ are groups and the above defines a homomorphism $H^i(G, A) \to H^i(G, B)$.

1.2. Commutative Cohomology. Let G be a group and A an abelian G-group. Then we call A a G-module. The same notation $A^G = \{a \in A \mid ga = a \ \forall g \in G\}$ represents the subgroup of elements in A fixed by G. A short exact sequence (written additively with the arrows G-homomorphisms)

$$0 \longrightarrow A \longrightarrow B \longrightarrow C \longrightarrow 0$$

of G-modules induces an exact sequence

$$0 \longrightarrow A^G \longrightarrow B^G \longrightarrow C^G$$

which in general cannot be extended to a long exact sequence.

Let $C^n(G, A), n \geq 0$ denote the set of all continuous maps from $G^n = G \times \cdots \times G$ (n copies) to A with $C^0(G, A) = A$. The elements of $C^n(G, A)$ are called the *n-cochains* (of G with coefficients in A). Define the n^{th} *coboundary* homomorphism

$$d_n\colon C^n(G, A) \longrightarrow C^{n+1}(G, A)$$

by the usual map [**7**]

$$\begin{aligned} d_n(f)(g_1,\dots,g_{n+1}) =& g_1 \cdot f(g_2,\dots,g_{n+1}) \\ &+ \sum_{i=1}^{n}(-1)^i f(g_1,\dots,g_{i-1},g_ig_{i+1},g_{i+2},\dots,g_{n+1}) \\ &+ (-1)^{n+1} f(g_1,\dots g_n). \end{aligned}$$

The composition of any two consecutive maps $d_{n+1} \circ d_n$ is zero.

PROOF. Here we show statement is true for $d_2 \circ d_1$.

$$\begin{aligned} d_2f(g_1,g_2,g_3) &= g_1 \cdot d_2f(g_2,g_3) - d_1f(g_1g_2,g_3) + d_1f(g_1,g_2g_3) - d_1f(g_1g_2) \\ &= g_1\big[g_2f(g_3) - f(g_2g_3) + f(g_2)\big] - \big[g_1g_2f(g_3) - f(g_1g_2g_3) + f(g_1g_2)\big] \\ &\quad + \big[g_1f(g_2g_3) - f(g_1g_2g_3) + f(g_1)\big] - \big[g_1f(g_2) - f(g_1g_2) + f(g_1)\big] \\ &= 0 \end{aligned}$$

□

There is a sequence $0 \to C^0(G,A) \to C^1(G,A) \to C^2(G,A) \to \cdots$ which we call a cochain complex.

Definition 1.4. Let $Z^n(G,A) = \ker d_n$. The elements of this group are called *n-cocycles*. Let $B^n(G,A) = \text{image } d_{n-1}$ with $B^0(G,A) = \{0\}$. The elements of this group are called *n-coboundaries*.

Since $d_{n+1} \circ d_n = 0$, image $d_n \subset \ker d_{n+1}$ so $B^n(G,A)$ is always a subgroup of $Z^n(G,A)$ and we can consider the quotient group.

Definition 1.5. For any G-module A the quotient group $Z^n(G,A)/B^n(G,A)$ is called the n^{th} *cohomology group of* G *in* A and is denoted by $H^n(G,A),\ n \geq 0$.

Notice that the cohomology sets $H^0(G,A)$ and $H^1(G,A)$ coincide for A abelian and non-abelian. Identify $f \in C^0(G,A)$ with an element of A by writing $a = f(0)$. We have $d_0(f)(g) = ga - a$. Thus $a \in Z^0(G,A)$ if and only if for all $g \in G, ga = a$. In other words, $Z^0(G,A) = A^G$ so

$$H^0(G,A) = \frac{Z^0(G,A)}{B^0(G,A)} = A^G$$

for any group G and G-module A.

Given $f \in C^1(G,A)$ we have $d_1(f)(g_1,g_2) = g_1 \cdot f(g_2) - f(g_1g_2) + f(g_1)$. So $f \in Z^1(G,A)$ if and only if $f(g_1g_2) = g_1f(g_2) + f(g_1)$. This is called the *1-cocycle* condition and we have that f is a *1-coboundary* $f \in B^1(G,A)$ if and only if there is an $a \in A$ such that f satisfies, $f(g) = ga - a$. Two 1-cocycles are *equivalent* if they differ by a 1-coboundary. The first cohomology group

$$H^1(G,A) = \frac{Z^1(G,A)}{B^1(G,A)}$$

is the group of equivalence classes of 1-cocycles. Since 1-cocycles are crossed homomorphisms and 1-coboundaries are principle crossed homomorphisms some may call the first cohomology group the equivalence classes of crossed homomorphisms [**9**].

When $f \in C^2(G,A)$ we have

$$d_2(f)(g_1,g_2,g_3) = g_1 \cdot f(g_2,g_3) - f(g_1g_2,g_3) + f(g_1,g_2g_3) - f(g_1,g_2)$$

so $f \in Z^2(G, A)$ if and only if $0 = g_1 \cdot f(g_2, g_3) - f(g_1 g_2, g_3) + f(g_1, g_2 g_3) - f(g_1, g_2)$ which is to say

$$g_1 \cdot f(g_2, g_3) + f(g_1, g_2 g_3) = f(g_1 g_2, g_3) + f(g_1, g_2).$$

This is called the *2-cocycle* condition. Does this look familiar? Written multiplicatively this is the condition (‡) required of our factor sets above. The functions $f \in B^2(G, A)$ are the image under d_1 and the *2-coboundaries*. Two 2-cocycles are *equivalent* if they differ by a 2-coboundary, therefore

$$H^2(G, A) = \frac{Z^2(G, A)}{B^2(G, A)}$$

is the set of equivalence classes of 2-cocycles. Considering the case when K/F is a Galois extension $G = \mathrm{Gal}(K/F)$ and $A = K^\times$, there is a bijection $\psi \colon H^2(G, K^\times) \to Br(K/F)$, defined by $\psi(f) = [(K, G, f)]$ which can be shown to be a homomorphism by the next proposition [**2**][**7**].

Proposition 1.1. *If K/F is a Galois extension with Galois group G, and if $f = \{f_{\sigma,\tau}\}$ and $g = \{g_{\sigma,\tau}\}$ are factor sets then $\psi(f)\psi(g) = \psi(fg)$ which is to say*

$$[(K, G, f)][(K, G, g)] = [(K, G, fg)].$$

A proof can be found in [**2**] on pages 126-128. Given $A = [(K, G, f)], B = [(K, G, g)]$ and $C = [(K, G, c)], c = fg$ the idea is to show that $A \otimes_F B$ is equivalent to C as a finite dimensional central simple F-algebra.

2. The Long and Short of Exact Sequences

Let A, B and C be abelian G-modules and consider the short exact sequence

$$1 \to A \xrightarrow{i} B \xrightarrow{j} C \to 1.$$

There is a long exact sequence of abelian groups

$$1 \to H^0(G,A) \xrightarrow{i} H^0(G,B) \xrightarrow{j} H^0(G,C) \xrightarrow{\delta_0} H^1(G,A) \xrightarrow{i} H^1(G,B) \xrightarrow{j}$$
$$H^1(G,C) \xrightarrow{\delta_1} \cdots \xrightarrow{\delta_{n-1}} H^n(G,A) \xrightarrow{i} H^n(G,B) \xrightarrow{j} H^n(G,C) \xrightarrow{\delta_n} \cdots$$

We are going to explain the homomorphisms connecting the cohomology groups.

2.1. The connecting map δ. The map $i\colon H^n(G,A) \to H^n(G,B)$ is defined by $f_n(g_1,\dots,g_n) \mapsto i\big(f_n(g_1,\dots,g_n)\big)$ and $j\colon H^n(G,B) \to H^n(G,C)$ is defined by $f_n(g_1,\dots,g_n) \mapsto j\big(f_n(g_1,\dots,g_n)\big)$. But what is $\delta_n\colon H^n(G,C) \to H^{n+1}(G,A)$, the connecting map between the cohomology groups?

In general define $\delta_n\colon H^n(G,C) \to H^{n+1}(G,A)$, $\delta_n(f_n)(g_1,\dots,g_n) = f_{n+1}(g_1\dots,g_{n+1})$ by the following. Given $f_n \in H^n(G,C)$ consider the function as $f_n \in C^n(G,C)$. Choose a lift $\tilde{f}_n \in C^n(G,B)$ by the surjectivity of $B \to C$. Now apply the map d_n to get a function $d_n(\tilde{f}_n) \in C^{n+1}(G,B)$. One can check that $j(d_n(\tilde{f}_n)) = 0$ so so in fact we have $d_n(\tilde{f}_n) \in C^{n+1}(G,A)$. Now with this we can take $\delta_n(f_n) = d_n(\tilde{f}_n) = f_{n+1}$.

Now we will explicitly compute δ_0. As we did above identify $f \in H^0(G,C)$ with $c \in C^G$, $f \in H^0(G,B)$ with $b \in B^G$ and define $\delta_0(c) \doteq f_1$ with $c = j(b)$ and $f_1 \in H^1(G,A)$.

Proposition 2.1. *The connecting map δ_0 is a well-defined homomorphism whose image satisfies the 1-cocycle condition.*

PROOF. (1) $\delta : H^0(G, C) \to H^1(G, A)$. We must show $f_1(g) = gb - b \in A$. If this is true, then the image is in the kernel of j. Applying j,

$$j(f_1(g)) = j(gb - b) = j(gb) - j(b) = g(j(b)) - j(b) = g(c) - c = c - c = 0$$

where moving g follows from j being a G-module homomorphism.

(2) δ is well-defined. Let $b' \in B$ such that $j(b') = c$. Then $j(b'-b) = j(b')-b(b) = c - c = 0$ when means $b' - b \in \ker(j)$ and $b' - b \in \text{image}(i)$ by exactness. There exists an $a \in A$ such that $a + b = b'$. Let $f_1'(g) = gb' - b'$ Then

$$f_1(g) - f_1'(g) = gb - b - gb' + b' = g(b - b') - (b - b') = ga - a = 0$$

so $f_1 = f_1'$.

(3) δ is a homomorphism. Write $\delta_0(f + f') = \delta(c+c')$ with $f_1 = \delta_0(c+c')$. Then

$$\begin{aligned} f_1(g) &= g(b + b') - (b + b') \\ &= g(b) + g(b') - b - b' \\ &= g(b) - b + g(b') - b' \\ &= f_1(g) + f_1'(g) \end{aligned}$$

Which shows $\delta_0(f + f') = \delta_0(f) + \delta_0(f')$.

(4) δ is a 1-cocycle. By definition $f_1(g_1g_2) = g_1g_2(b) - b = g_1g_2(b) - b + \big(g_1(b) - g_1(b)\big) = g_1(g_2(b) - b) + g_1(b) - b = g_1f_1(g_2) + f_1(g_1)$.

(5) $\ker(\delta) = \mathrm{Im}(j)$. Let $c \in \mathrm{Im}(j)$. There exists $b \in B$ such that $j(b) = c$. This choice of b is not unique as we've seen so $\delta_0(c) \doteq f_1$. Thus $f_1(g) = g(b) - b = b - b = 0$ shows $\ker(\delta) \supset \mathrm{Im}(j)$. Now $c \in \ker(\delta)$ means $f_1(g) = gb - b$ is a 1-coboundary. Thus there exists an $a \in A$ such that $f_1(g) = ga - a$. Then

$$ga - a = gb - b$$

$$ga - gb = a - b$$

$$g(a - b) = b - a \quad \in H^0(G, B)$$

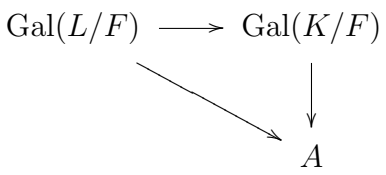
So we can choose a lift of c, $b' = b - a$. This is indeed a lift because $j(b') = j(b - a) = j(b) - j(a) = c - 0 = c$. Then $f_1(g) = g(b') - b' = 0$. □

2.2. The Inflation Homomorphism. Suppose H is a normal subgroup of G and A is a G-module. The group A^H is a G/H-module under the action defined by $(gH) \cdot a = ga$. It follows that the projection $\varphi\colon G \to G/H$ and the inclusion $\psi\colon A^H \to A$ makes ψ a G-module homomorphism via $\psi(\varphi(g')a = g'\psi(a)$ for all $g' \in G/H$ and $a \in A$, making A a G/H-module [**1**]. The corresponding group homomorphism on cohomology is called the *inflation homomorphism*

$$Inf\colon H^n(G/H, A^H) \to H^n(G, A), \quad n \geq 0.$$

In particular, consider the tower of fields $F \subset K \subset L$, K/F and L/F both Galois and suppose $\mathrm{Gal}(L/K)$ is normal in $\mathrm{Gal}(L/F)$. The quotient is isomorphic to

$\mathrm{Gal}(K/F)$ since $K = L^{\mathrm{Gal}(L/K)}$. Given a G-module A, we may construct the diagram



and the corresponding inflation homomorphism

$$Inf\colon H^n(\mathrm{Gal}(K/F), A) \to H^n(\mathrm{Gal}(L/F), A).$$

CHAPTER 3

The Principal Result

1. Kummer Theory and the Det Map

Let $V \simeq \mathbb{Q}^n$ and (V, Q_1) and (V, Q_2) be non-degenerate quadratic spaces over $\mathbb{Q}$ of the same rank. By Theorem 3.1 and its corollary there exists a finite extension $K/\mathbb{Q}$ such that

$$V_1 \otimes_{\mathbb{Q}} K \simeq V_2 \otimes_{\mathbb{Q}} K$$

as quadratic spaces. Recall that Theorem 4.6 tells us that any element $[S] \in Br(K/\mathbb{Q})$ has a unique representative S containing K as a maximal subfield, and if we choose $K/\mathbb{Q}$ to be Galois, K will split S. For any tower of fields $\mathbb{Q} \subset K \subset L$ with K and L finite and Galois over F with Galois groups $\mathrm{Gal}(K/\mathbb{Q})$ and $\mathrm{Gal}(L/\mathbb{Q})$ respectively, the diagram

$$\begin{array}{ccc} H^2(\mathrm{Gal}(K/\mathbb{Q}), K^\times) & \xrightarrow{Inf} & H^2(\mathrm{Gal}(L/\mathbb{Q}), L^\times) \\ \downarrow & & \downarrow \\ Br(K/F) & \xrightarrow{\varphi} & Br(L/F) \end{array}$$

commutes. The vertical arrows are defined by $f \mapsto [(K, G, f)]$ as stated earlier and φ is an injection. Using inflation and the fact that $Br(F) = \bigcup Br(K/F)$ one can show that for any separable algebraic closure $\overline{\mathbb{Q}}$ of $\mathbb{Q}$ there is a canonical isomorphism $Br(\mathbb{Q}) \to H^2(\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}), \overline{\mathbb{Q}}^\times)$ [**5**].

We are interested in studying "how far apart" or different these quadratic forms are by examining the behavior of the Galois group on the isomorphism. Let $K/\mathbb{Q}$ be as described above. We can express this isomorphism as a matrix $\Phi \in \mathrm{GL}_n(K)$, $\Phi\colon A_1 \to A_2$, such that

$$\Phi^t A_1 \Phi = A_2$$

where A_1 and A_2 are the associated matrices of the quadratic spaces respectively. If V_1 and V_2 were already isomorphic over $\mathbb{Q}$ then we can choose $\Phi \in \mathrm{GL}_n(\mathbb{Q})$; so the question is, *"How far is* Φ *from having rational entries?"*.

Let $G = \mathrm{Gal}(K/\mathbb{Q})$ and define a function

$$c_\sigma \in Z^1\big(G, \mathcal{O}_{Q_2}(K)\big)$$

by

$$c_\sigma = \sigma(\Phi)\Phi^{-1}. \tag{3}$$

The matrix Φ is not unique; if we replace Φ by $T\Phi$, $T \in \mathcal{O}_{Q_2}(K)$, then we have

$$c'_\sigma = \sigma(T\Phi)(T\Phi)^{-1} = \sigma(T)\sigma(\Phi)\Phi^{-1}T^{-1} = \sigma(T)c_\sigma T^{-1}$$

showing the new 1-cocycle $c'_\sigma \in Z^1\big(G, \mathcal{O}_{Q_2}(K)\big)$ differs from c_σ by a 1-coboundary, $\sigma(T)T^{-1} \in B^1\big(G, \mathcal{O}_{Q_2}(K)\big)$. Let $[c_\sigma]$ denote an equivalence class of 1-cocycles modulo 1-coboundaries in order to write $[c_\sigma] \in H^1\big(G, \mathcal{O}_{Q_2}(K)\big)$. If we can choose $\Phi \in \mathrm{GL}_n(\mathbb{Q})$ then $[c_\sigma] \in H^1\big(G, \mathcal{O}_{Q_2}(K)\big)$ is the identity element. The following theorem explains

that there is an isomorphism between K-equivalent quadratic spaces on V and the elements of the cohomology class $H^1\big(G, \mathcal{O}_{Q_2}(K)\big)$. For a proof see page 244 of [**8**]

Theorem 1.1. *The equivalence classes of quadratic forms Q_2 on V which are K-equivalent to Q_1 are in bijective correspondence with the elements of $H^1(G, \mathcal{O}_{Q_2}(K))$. The class of Q_1 corresponds to the identity element.*

Given a 1-cocycle $c_\sigma = \sigma(\Phi)\Phi^{-1}$ we can consider its determinant which will be either ± 1 and the homomorphism $\det c_\sigma$ will be yield a cohomology class $[\det c_\sigma] \in H^1\big(G, \mu_2\big)$ where $\mu_2 = \{\zeta \in \mathbb{C}^\times : \zeta^2 = 1\}$.

Now, consider the short exact sequence

$$1 \longrightarrow \mu_n \longrightarrow K^\times \xrightarrow{x \mapsto x^n} K^\times \longrightarrow 1$$

and pass to cohomology to get the long exact sequence

$$1 \to H^0(G, \mu_n) \to H^0(G, K^\times) \to H^0(G, K^\times) \xrightarrow{\text{kum}} H^1(G, \mu_n) \to H^1(G, K^\times) \to \cdots .$$

Galois groups stabilize the base field so by definition $H^0(G, \mu_n) = \mu_n$, $H^0(G, K^\times) = K^\times$. Hilbert's Theorem 90 will show that $H^1(G, K^\times)$ is trivial.

Theorem 1.2 (Hilbert's Theorem 90)**.** *Let K/F be a finite Galois extension and $G =$Gal(K/F). Then $H^1(G, K^\times) = 1$.*

Proof. Let $f \in Z^1(G, K^\times)$. For all $\sigma \in G$ let $\alpha_\sigma = f(\sigma)$. Because automorphisms are linearly independent there exists $\gamma \in K$ such that

$$\beta = \sum_{\tau \in G} \alpha_\tau \tau(\gamma)$$

with $\beta \in K^\times$. For any $\sigma \in G$

$$\sigma(\beta) = \sum_{\tau \in G} \sigma(\alpha_\tau)\sigma\tau(\gamma) = \alpha_\sigma^{-1} \sum_{\tau \in G} \alpha_{\sigma\tau}\sigma\tau(\gamma) = \alpha_\sigma^{-1}\beta.$$

This means that $\alpha_\sigma = \beta\sigma(\beta)^{-1}$ which is the 1-coboundary condition for an element $a = \beta^{-1}$ and this means that every 1-cocycle is a 1-coboundary and therefore $H^1(G, K^\times) = 1$ [**1**]. □

Thus, we may write the exact sequence

$$1 \longrightarrow \mu_n \longrightarrow \mathbb{Q}^\times \xrightarrow{x \mapsto x^n} \mathbb{Q}^\times \xrightarrow{\text{kum}} H^1(G, \mu_n) \longrightarrow 1.$$

What about the connecting map "kum"? We will describe this map explicitly [**8**].

Theorem 1.3. *The Kummer map is the map*

$$\mathbb{Q}^\times/(\mathbb{Q}^\times)^n \xrightarrow{\sim} H^1(G, \mu_n)$$

defined by

$$kum_a(\sigma) = \frac{\sigma(\sqrt[n]{a})}{\sqrt[n]{a}}$$

for $a \in \mathbb{Q}^\times/(\mathbb{Q}^\times)^n$ where $\sqrt[n]{a} \in K^\times$ is a primitive n^{th} root of a.

Proof. This is the formula for the connecting map δ_0 in this particular case. □

This is an isomorphism because exactness tells us the Kummer map is surjective with $\ker(\text{kum}) = \mu_2$.

Proposition 1.4. *For any given $a \in \mathbb{Q}^\times/(\mathbb{Q}^\times)^n$, the Kummer map is well-defined.*

PROOF. Saying that Kummer is well-defined is equivalent to saying that different choices of n^{th} roots of a changes Kummer by a 1-coboundary. Let $\zeta = \sqrt[n]{a}$ be another primitive n^{th} root. Then for $1 < b \leq n$

$$\mathrm{kum}_a(\sigma) = \frac{\sigma(\zeta^b)}{\zeta^b} = \frac{\sigma(\zeta\zeta^{b-1})}{\zeta\zeta^{b-1}} = \frac{\sigma(\zeta)}{\zeta} \cdot \frac{\sigma(\zeta^{b-1})}{\zeta^{b-1}}$$

and $\sigma(\zeta^{b-1})/\zeta^{b-1} \in \mu_n$ is a 1-coboundary. □

We summarize the above results in the next theorem.

Theorem 1.5. *Let (V, Q_1) and (V, Q_2) be nondegenerate n dimensional quadratic spaces over $\mathbb{Q}$. Let $K/\mathbb{Q}$ be the field extension where (V, Q_1) and (V, Q_2) become isomorphic. Let $d(Q_1)d(Q_2) = a \in \mathbb{Q}^\times/(\mathbb{Q}^\times)^2$. Then $kum_a(\sigma) = \det c_\sigma$ where $kum_a(\sigma)$ and c_σ are described as above.*

PROOF. By Corollary 1.2 above we can always find an orthogonal basis for Q_1 and Q_2, so without loss of generality let

$$A_1 = \begin{bmatrix} d_1 & & & \\ & d_2 & & \\ & & \ddots & \\ & & & d_n \end{bmatrix} \quad \text{and} \quad A_2 = \begin{bmatrix} b_1 & & & \\ & b_2 & & \\ & & \ddots & \\ & & & b_n \end{bmatrix}$$

with the $d_i, b_i \in \mathbb{Q}^\times$ be the associated matrices of Q_1 and Q_2 respectively. Take $K = \mathbb{Q}(\sqrt{d_1}, \ldots, \sqrt{d_n}, \sqrt{b_1}, \ldots, \sqrt{b_n})$. Choose an isomorphism $\Phi \in \mathrm{GL}_n(K)$ such

that $\Phi\colon A_1 \to A_2$ defined by $\Phi^t A_1 \Phi = A_2$ gives

$$\Phi = \begin{bmatrix} \frac{\sqrt{d_1}}{\sqrt{b_1}} & & & \\ & \frac{\sqrt{d_2}}{\sqrt{b_2}} & & \\ & & \ddots & \\ & & & \frac{\sqrt{d_n}}{\sqrt{b_n}} \end{bmatrix}$$

with inverse matrix

$$\Phi^{-1} = \begin{bmatrix} \frac{\sqrt{b_1}}{\sqrt{d_1}} & & & \\ & \frac{\sqrt{b_2}}{\sqrt{d_2}} & & \\ & & \ddots & \\ & & & \frac{\sqrt{b_n}}{\sqrt{d_n}} \end{bmatrix}.$$

For all $\sigma \in G$ let $c_\sigma \in H^1\big(G, \mathcal{O}_{Q_2}(K)\big)$ be as in (3). Then

$$\begin{aligned} c_\sigma &= \sigma(\Phi)\Phi^{-1} \\ &= \begin{bmatrix} \sigma\left(\frac{\sqrt{d_1}}{\sqrt{b_1}}\right) & & & \\ & \sigma\left(\frac{\sqrt{d_2}}{\sqrt{b_2}}\right) & & \\ & & \ddots & \\ & & & \sigma\left(\frac{\sqrt{d_n}}{\sqrt{b_n}}\right) \end{bmatrix} \begin{bmatrix} \frac{\sqrt{b_1}}{\sqrt{d_1}} & & & \\ & \frac{\sqrt{b_2}}{\sqrt{d_2}} & & \\ & & \ddots & \\ & & & \frac{\sqrt{b_n}}{\sqrt{d_n}} \end{bmatrix} \\ &= \begin{bmatrix} \sigma\left(\frac{\sqrt{d_1}}{\sqrt{b_1}}\right)\frac{\sqrt{b_1}}{\sqrt{d_1}} & & & \\ & \sigma\left(\frac{\sqrt{d_2}}{\sqrt{b_2}}\right)\frac{\sqrt{b_2}}{\sqrt{d_2}} & & \\ & & \ddots & \\ & & & \sigma\left(\frac{\sqrt{d_n}}{\sqrt{b_n}}\right)\frac{\sqrt{b_n}}{\sqrt{d_n}} \end{bmatrix} \end{aligned}$$

$$= \begin{bmatrix} \mathrm{kum}_{d_1/b_1}(\sigma) & & & \\ & \mathrm{kum}_{d_2/b_2}(\sigma) & & \\ & & \ddots & \\ & & & \mathrm{kum}_{d_n/b_n}(\sigma) \end{bmatrix}.$$

Then $\det c_\sigma = \mathrm{kum}_{d(Q_1)d(Q_2)}(\sigma)$. □

2. Clifford and Hasse

We can also use Galois Cohomology to recover the Hasse invariant, following Springer's construction in [**8**]. Recall that the Clifford group $\Gamma_Q(K)$ of the quadratic space (V, Q) consists of the invertible elements t of the Clifford algebra $C(V, Q)$ such that $\gamma(t)V = Vt$, and that there is a short exact sequence

$$1 \to K^\times \to \Gamma_Q(K) \to \mathcal{O}_Q(K) \to 1.$$

We can pass to cohomology to get a long exact sequence and we will focus on the connecting map between the first and second cohomology groups

$$\cdots \to H^1\big(G, \mathcal{O}_Q(K)\big) \xrightarrow{\text{clif}} H^2\big(G, K^\times\big) \to \cdots$$

which we will call "clif". Chapter 2 showed that when K/F is Galois, $H^2\big(G, K^\times\big) \simeq Br(K/F)$. The map clif is given as follows. Let $c_\sigma \in Z^1\big(G, \mathcal{O}_Q(K)\big)$. By the surjectivity of $\Gamma_Q(K) \to \mathcal{O}_Q(K)$ we can choose, for every $\sigma \in \mathrm{Gal}(K/F)$, a lift $s_\sigma \in \Gamma_Q(K)$ of c_σ. Then for all $x \in V$, $\sigma \in G$, s_σ satisfies [**4**][**8**]

$$c_\sigma(x) = \gamma(s_\sigma) x s_\sigma^{-1}. \tag{4}$$

Define a 2-cocycle $a_{\sigma,\tau} \in Z^2(G, K^\times)$ using the relation † above by

$$a_{\sigma,\tau} = s_{\sigma\tau} s_\tau^{-1} s_\sigma^{-1} \in K^\times. \tag{5}$$

The class of $a_{\sigma,\tau} \in H^2(G, K^\times)$ depends only on the class of $c_\sigma \in H^1(G, K^\times)$ and not on the lift s_σ. Therefore, we have a class

$$\mathrm{clif}(c) = [a_{\sigma,\tau}] \in H^2\big(G, K^\times\big).$$

One can show that this equivalence class has order 1 or 2 [**8**].

Our goal is to construct $\mathrm{clif}(c)$ in terms of an expression which we will define to be the Hasse invariant of a quadratic form over $\mathbb{Q}$. Take Q_1 and Q_2 as in the start of the chapter with orthogonal bases and $\Phi\colon A_1 \mapsto A_2$. Then $c_\sigma = \sigma(\Phi)\Phi^{-1} \in H^1\big(G, \mathcal{O}_{Q_2}(K)\big)$ is diagonal. Let $\lambda_i = \sqrt{d_i}/\sqrt{b_i}$ and define $\varepsilon_i(\sigma) \in \{0, 1\}$ by the relation $\sigma\lambda_i = (-1)^{\varepsilon_i(\sigma)}\lambda_i$ for all $\sigma \in G$. Then $c_\sigma(e_i) = (-1)^{\varepsilon_i(\sigma)} e_i$ where e_i is the i^{th} standard basis vector. By definition $\sigma\tau\lambda_i = (-1)^{\varepsilon_i(\sigma\tau)}\lambda_i$. But also, $\sigma\tau\lambda_i = \sigma(\tau\lambda_i) = (-1)^{\varepsilon_i(\tau)}(-1)^{\varepsilon_i(\sigma)}\lambda_i$. Therefore,

$$\varepsilon_i(\sigma\tau) \equiv \varepsilon_i(\tau) + \varepsilon_i(\sigma) \pmod 2.$$

Recall the function $\alpha(t)(x)$ defined in (2) and notice that this is just (4) with $t = s_\sigma$. We have $\alpha(e_i)(x) = -e_i x e_i^{-1}$ for all $x, e_i \in V$. Using the fact that $\rho\colon V \to C(V, Q_2)$ has the property $\rho(x)\rho(e_i) + \rho(e_i)\rho(x) = 2\langle x, e_i\rangle_{Q_2}$, one can see that $\alpha(e_i)(x)$ is the

reflection of x in the orthogonal hyperplane to e_i, via the calculation

$$\begin{aligned} -\alpha(e_i)(x) &= (-xe_i + 2\langle x, e_i\rangle)e_i^{-1} \\ &= \big(-xe_i + 2\langle x, e_i\rangle\big)\frac{e_i}{Q_2(e_i)} \\ &= -\left(x - \frac{2\langle x, e_i\rangle}{Q_2(e_i)}e_i\right). \end{aligned}$$

For $e_i, e_j \in V$, $\alpha(e_i)(e_i) = -e_i$ and $\alpha(e_i)(e_j) = e_j$. This means that if $\sigma(\lambda_i) = -\lambda_i$ and σ fixes all other $\lambda_j (j \neq i)$, a lift of c_σ is $s_\sigma = e_i$. Suppose now that σ moves λ_i, λ_j and fixes all other $\lambda_k, (k \neq i, j)$. Since the map is a ring homomorphism we find that a lift of c_σ is $s_\sigma = e_ie_j$ as confirmed by the calculations $\alpha(e_ie_j)(e_i) = -e_i, \alpha(e_ie_j)(e_j) = -e_j$ and $\alpha(e_ie_j)(e_k) = e_k$. Let $s_\sigma = e_1^{\varepsilon_1(\sigma)} \cdots e_n^{\varepsilon_n(\sigma)}$. Then s_σ is a lift of c_σ for all $\sigma \in G$. We will now compute an explicit formula for $a_{\sigma,\tau} \in Z^2(G, K^\times)$ from (5) using this lift:

$$\begin{aligned} a_{\sigma,\tau} &= s_{\sigma\tau}s_\tau^{-1}s_\sigma^{-1} \\ &= e_1^{\varepsilon_1(\sigma\tau)} \cdots e_n^{\varepsilon_n(\sigma\tau)} \cdot \left[e_1^{\varepsilon_1(\tau)} \cdots e_n^{\varepsilon_n(\tau)}\right]^{-1} \cdot \left[e_1^{\varepsilon_1(\sigma)} \cdots e_n^{\varepsilon_n(\sigma)}\right]^{-1} \\ &= e_1^{\varepsilon_1(\sigma\tau)} \cdots e_n^{\varepsilon_n(\sigma\tau)} e_n^{-\varepsilon_n(\tau)} \cdots e_1^{-\varepsilon_1(\tau)} e_n^{-\varepsilon_n(\sigma)} \cdots e_1^{-\varepsilon_1(\sigma)} \end{aligned} \tag{6}$$

Here we must be careful because via the relation $e_ie_j = -e_je_i$ we will pick up -1's that depend on how elements are permuted. Consider moving $e_n^{-\varepsilon_n(\sigma)}$ to the left before $e_n^{-\varepsilon_n(\tau)}$. If $\varepsilon_n(\sigma) = 0$ then $e_n^{-\varepsilon_i(\sigma)} = 1$. So suppose $\varepsilon_n(\sigma) = 1$. Then if for any of the intermediate terms $e_i^{-\varepsilon(\tau)}$ we have $\varepsilon_i(\tau) = 0$, we do not pick up a negative when we permute it with $e_n^{-\varepsilon_n(\sigma)}$. After moving $e_n^{-\varepsilon_n(\sigma)}$ directly in front of $e_n^{-\varepsilon_n(\tau)}$ the product

$e_n^{\varepsilon_n(\sigma\tau)} e_n^{-\varepsilon_n(\sigma)} e_n^{-\varepsilon_n(\tau)}$ is simply $e_n^{\varepsilon_n(\sigma\tau)-\varepsilon_n(\sigma)-\varepsilon_n(\tau)} \in K^\times$ and thus by commutativity can be moved to the end of the expression without picking up any negative signs. The element $e_n^{\varepsilon_n(\sigma\tau)-\varepsilon_n(\sigma)-\varepsilon_n(\tau)}$ is in fact in $K^\times$ because if $\varepsilon_n(\tau) = 0$ then $\varepsilon_n(\sigma\tau) = 1$ and we have $e_n^0 = 1$. Otherwise if $\varepsilon_n(\tau) = 1$ then $\varepsilon_n(\sigma\tau) = 0$ and we have $e_n^{-2} = d_n$. Thus moving $e_n^{-\varepsilon_n(\sigma)}$ as we have described above gives the following relation for (6)

$$a_{\sigma,\tau} = \prod_{i<n} (-1)^{\varepsilon_i(\tau)\epsilon_n(\sigma)} e_1^{\varepsilon_1(\sigma\tau)} \cdots e_{n-1}^{\varepsilon_{n-1}(\sigma\tau)} e_{n-1}^{-\varepsilon_{n-1}(\tau)} \cdots$$
$$\cdots e_1^{-\varepsilon_1(\tau)} e_{n-1}^{-\varepsilon_{n-1}(\sigma)} \cdots e_1^{-\varepsilon_1(\sigma)} \prod_{\varepsilon_n(\tau)=\varepsilon_n(\sigma)=1} d_n$$

Now we move $e_{n-1}^{-\varepsilon_{n-1}(\sigma)}$ in the same manner and see that we pick up

$$\prod_{i<n-1} (-1)^{\varepsilon_i(\tau)\varepsilon_{n-1}(\sigma)}$$

and will have d_{n-1} at the end if $\varepsilon_{n-1}(\sigma) = \varepsilon_{n-1}(\tau) = 1$. Continuing this process we have a new equation for $a_{\sigma,\tau} \in Z^2(G, K^\times)$

$$a_{\sigma,\tau} = \prod_{i<j} (-1)^{\varepsilon_i(\tau)\varepsilon_j(\sigma)} \prod_{\varepsilon_i(\tau)=\varepsilon_i(\sigma)=1} d_i. \tag{7}$$

We are going to define two new cohomology classes for two different cocycles. Given these new cohomology classes we will deduce a specific relationship between them and $[a_{\sigma,\tau}]$. Let $K/\mathbb{Q}$ Galois, and let $d, b \in \mathbb{Q}^\times$. Choose square roots $\sqrt{d}, \sqrt{b} \in K$. For any $\sigma \in G$ we have

$$\sigma(\sqrt{d}) = (-1)^{d(\sigma)}\sqrt{d} \tag{8}$$
$$\sigma(\sqrt{b}) = (-1)^{b(\sigma)}\sqrt{b}.$$

where $d(\sigma), b(\sigma) \in \{0, 1\}$. With these relations define $(d, b) \in H^2(G, K^\times)$ to be the cohomology class of the 2-cocycle

$$f_{\sigma,\tau} = (-1)^{d(\sigma)b(\tau)} \in K^\times \tag{9}$$

for all $\sigma, \tau \in \mathrm{Gal}(K/\mathbb{Q})$. The class (d, b) depends on K but if L/K is Galois then the lift from K to L of (d, b) is the class $(d, b) \in H^2(\mathrm{Gal}(L/\mathbb{Q}), L^\times)$. By definition (d, b) is symmetric and multiplicative in d and b [**8**]. In fact, (d, b) is the Hilbert Symbol.

Now define $\{d, b\} \in H^2(G, K^\times)$ to be the cohomology class of the 2-cocycle

$$g_{\sigma,\tau} = \begin{cases} b & \text{if } \sigma\sqrt{d} = -\sqrt{d}, \tau\sqrt{d} = -\sqrt{d} \\ 1 & \text{otherwise} \end{cases} \tag{10}$$

Combining the last product of (7) with (10) gives

$$[a_{\sigma,\tau}] = \prod_{i<j} (-1)^{\varepsilon_i(\tau)\varepsilon_j(\sigma)} \prod_{i=1}^{n} \{d_i b_i, d_i\}$$

because $\varepsilon_i(\sigma) = \varepsilon_i(\tau) = 1$ means by definition that $\sigma\left(\sqrt{d_i}\sqrt{b_i}\right) = -\sqrt{d_i}\sqrt{b_i}$ and $\tau\left(\sqrt{d_i}\sqrt{b_i}\right) = -\sqrt{d_i}\sqrt{b_i}$ for all $\sigma, \tau \in G$. Using (8) above we see that $d_i b_i(\sigma) = \varepsilon_i(\sigma)$ thus using (9) we rewrite the first product in (7) as

$$[a_{\sigma,\tau}] = \prod_{i<j} (d_i b_i, d_j b_j) \prod_{i=1}^{n} \{d_i b_i, d_i\}. \tag{11}$$

Proposition 2.1. *Let $\{d, b\} \in H^2(G, K^\times)$ be defined as in* (10) *and $(d, b) \in H^2(G, K^\times)$ be defined as in* (11)*. Then $\{d, b\} = (d, b)$.*

Proof. As long as $K/\mathbb{Q}$ is large enough to contain all the square roots these two classes are defined. This equality follows from the properties of the Hilbert Symbol

but we will follow Springer's [**8**] construction and use the above definitions. Let $n = 2$ and first take $d_1 = b_1 = 1, d_2 = d$ and $b_2 = b$. Then

$$[a_{\sigma,\tau}] = (1, db)\{1, 1\}\{db, d\} = \{db, d\}. \tag{12}$$

Now if we take $d_1 = d, d_2 = 1, b_1 = 1, b_2 = b$ then

$$[a_{\sigma,\tau}] = (d, b)\{d, d\}\{b, 1\} = (d, b)\{d, d\} \tag{13}$$

represents the same cohomology class. Putting (12) and (13) we get

$$\{db, d\} = (d, b)\{d, d\}$$

If $c = d$ then $\{d^2, d\} = (d, d)\{d, d\}$. By definition the left hand side is 1, therefore $\{d, d\} = (d, d)^{-1} = (d, d)$ giving

$$\{db, d\} = (d, b)(d, d) = (d, db) = (db, d)$$

which implies $\{d, b\} = (d, b)$. □

Recognizing that $(d, d) = \{d, -1\}$ we get

$$(d, -d)(d, -1) = (-1)^{d_\varepsilon(\sigma)-d_\varepsilon(\tau)}(-1)^{d_\varepsilon(\sigma)-1(\tau)} = (-1)^{d_\varepsilon(\sigma)d_\varepsilon(\tau)} \cdot 1 = (d, d) = (d, -1)$$

which shows that $(d, -d) = 1$. Thus, we may rewrite $[\alpha(\sigma, \tau)] \in H^2(G, K^\times)$ as (11) as

$$[a_{\sigma,\tau}] = \prod_{i<j}(d_i b_i, d_j b_j) \prod_{i=1}^{n}(d_i b_i, d_i). \tag{14}$$

Suppose we had $Q_1 = (V, I_n)$ with I_n the identity matrix in order to compare the quadratic form Q_2 with the identity. Simply take all $d_i = 1$ and (14) becomes

$$[a_{\sigma,\tau}] = \prod_{i<j}(b_i, b_j).$$

From this, we will define the Hasse invariant of a quadratic form over $\mathbb{Q}$.

Definition 2.1 (The Hasse invariant over $\mathbb{Q}$)**.** Let (V, Q) be a non degenerate quadratic space over $\mathbb{Q}$ of dimension n and e_i $(1 \leq i \leq n)$ an orthogonal basis of V such that $Q(e_i) = a_i$, $a_i \in \mathbb{Q}^\times$. Define the *Hasse invariant* of Q to be the number $\epsilon(Q) \in \{\pm 1\}$

$$\epsilon(Q) = \prod_{i\leq j}(a_i, a_j).$$

The Hasse invariant of $\mathbb{Q}$ is an element of $H^2(G, K^\times)$ but since $H^2(G, K^\times) \simeq Br(K/F)$ the Hasse invariant in an element in the relative Brauer group. This notion of the Hasse invariant over $\mathbb{Q}$ coincides with the notion of the Hasse invariant over $\mathbb{Q}_p$ because the class we defined above $(\ ,\ ) \in H^2(G, K^\times)$ has the same properties as the Hilbert symbol. By this definition, the Hasse invariant of Q_2 is $\epsilon(Q_2) = \prod_{i\leq j}(b_i, b_j)$ and from (14) we see that

$$\begin{aligned}
[a_{\sigma,\tau}] &= \prod_{i<j}(b_i, b_j)\prod_{i=1}^{n}(b_i^2, b_i^2) \\
&= \prod_{i\leq j}(b_i, b_j)\prod_{i=1}^{n}(b_i, b_i) \\
&= \epsilon(Q_2)\prod_{i=1}^{n}(b_i, -1)
\end{aligned}$$

$$[a_{\sigma,\tau}] = \epsilon(Q_2)(-1, d(Q_2)) \in H^2(G, K^\times). \tag{15}$$

We now simply state a theorem from [**8**] that will allow us to generalize (15) for any quadratic spaces.

Theorem 2.2. *If Q, Q_1, Q_2 are three quadratic forms on V, then*

$$[a_K(Q_1, Q_2)] = \big(d(Q)d(Q1), d(Q)d(Q_2)\big)[a_K(Q, Q_1)][a_K(Q, Q_2)].$$

The element $[a_K(Q, Q_i)]$ represents the equivalence class in $H^2(G, K^\times)$ of Q_i compared to Q and $[a_K(Q_1, Q_2)]$ represents the same for Q_2 compared to Q_1.

See the reference for a proof. It follows that if $Q = (V, I_n)$ for arbitrary quadratic forms Q_1 and Q_2 we have

$$[a_{\sigma,\tau}] = \big(d(Q_1), d(Q_2)\big)\epsilon(Q_1)\epsilon(Q_2) \in H^2(G, K^\times). \tag{16}$$

3. Example

Let (V, A_1) and (V, A_2) be two quadratic spaces of dimension 2 over $\mathbb{Q}$ with the associated matrices

$$A_1 = \begin{bmatrix} a & \\ & b \end{bmatrix} \qquad \text{and} \qquad A_2 = \begin{bmatrix} 1 & \\ & 1 \end{bmatrix}.$$

They are isomorphic over the Galois extension $K/\mathbb{Q}$, $K = \mathbb{Q}(\sqrt{a}, \sqrt{b})$. The change of basis matrix

$$\Phi = \begin{bmatrix} \sqrt{a} & \\ & \sqrt{b} \end{bmatrix} \in \mathrm{GL}_2(K),$$

so that we have

$$A_1 = \Phi^t A_2 \Phi.$$

The Galois group

$$G = \mathrm{Gal}(K/\mathbb{Q}) = \{\iota, \sigma, \tau, \sigma\tau\}$$

has automorphisms defined by

$$\begin{array}{llll} \iota\colon \sqrt{a} \mapsto \sqrt{a} & \sigma\colon \sqrt{a} \mapsto -\sqrt{a} & \tau\colon \sqrt{a} \mapsto \sqrt{a} & \sigma\tau\colon \sqrt{a} \mapsto -\sqrt{a} \\ \iota\colon \sqrt{b} \mapsto \sqrt{b} & \sigma\colon \sqrt{b} \mapsto \sqrt{b} & \tau\colon \sqrt{b} \mapsto -\sqrt{b} & \sigma\tau\colon \sqrt{b} \mapsto -\sqrt{b} \end{array}$$

with the fixed fields of subgroups

$$\begin{array}{ll} K^{\iota} = \mathbb{Q} & K^{\tau} = \mathbb{Q}(\sqrt{a}) \\ K^{\sigma} = \mathbb{Q}(\sqrt{b}) & K^{\sigma\tau} = \mathbb{Q}(\sqrt{a}\sqrt{b}). \end{array}$$

The inverse matrix is

$$\Phi^{-1} = \begin{bmatrix} \frac{1}{\sqrt{a}} & \\ & \frac{1}{\sqrt{b}} \end{bmatrix}$$

and we now calculate $\det c_\sigma$, and $\det c_\sigma$:

$$c_\iota = \iota(\Phi)\Phi^{-1} = \begin{bmatrix} 1 & \\ & 1 \end{bmatrix} \qquad \det c_\iota = 1$$

$$c_\sigma = \sigma(\Phi)\Phi^{-1} = \begin{bmatrix} -1 & \\ & 1 \end{bmatrix} \qquad \det c_\sigma = -1$$

$$c_\tau = \tau(\Phi)\Phi^{-1} = \begin{bmatrix} 1 & \\ & -1 \end{bmatrix} \qquad \det c_\tau = -1$$

$$c_{\sigma\tau} = \sigma\tau(\Phi)\Phi^{-1} = \begin{bmatrix} -1 & \\ & -1 \end{bmatrix} \qquad \det c_\sigma\tau = 1.$$

We could have instead calculated $\mathrm{kum}_{d(Q_1)d(Q_2)}(\sigma) = \mathrm{kum}_{ab}(\sigma)$ as shown:

$$\mathrm{kum}_{ab}(\iota) = \frac{\iota(\sqrt{a}\sqrt{b})}{\sqrt{a}\sqrt{b}} = 1$$

$$\mathrm{kum}_{ab}(\sigma) = \frac{\sigma(\sqrt{a}\sqrt{b})}{\sqrt{a}\sqrt{b}} = -1$$

$$\mathrm{kum}_{ab}(\tau) = \frac{\tau(\sqrt{a}\sqrt{b})}{\sqrt{a}\sqrt{b}} = -1$$

$$\mathrm{kum}_{ab}(\sigma\tau) = \frac{\sigma\tau(\sqrt{a}\sqrt{b})}{\sqrt{a}\sqrt{b}} = 1.$$

This verifies Theorem 1.5. We turn our attention to the Hasse invariant by computing the cohomology class $(a, b) \in H^2(G, K^\times)$. Computing $a(\sigma)$ and $b(\sigma)$ using (8) for all $\sigma \in G$ we have $a(\sigma) = 1, b(\tau) = 1, a(\sigma\tau) = 1, b(\sigma\tau) = 1$, with all others equal to 0,

giving the following values of the 2-cocycle $f_{\sigma,\tau}$ from (9), to compute the class (a, b).

$$\begin{array}{llll} f_{\iota,\iota} = 1 & f_{\sigma,\iota} = 1 & f_{\tau,\iota} = 1 & f_{\sigma\tau,\iota} = 1 \\ f_{\iota,\sigma} = 1 & f_{\sigma,\sigma} = 1 & f_{\tau,\sigma} = 1 & f_{\sigma\tau,\sigma} = 1 \\ f_{\iota,\tau} = 1 & f_{\sigma,\tau} = -1 & f_{\tau,\tau} = 1 & f_{\sigma\tau,\tau} = -1 \\ f_{\iota,\sigma\tau} = 1 & f_{\sigma,\sigma\tau} = -1 & f_{\tau,\sigma\tau} = 1 & f_{\sigma\tau,\sigma\tau} = -1. \end{array}$$

We also compute the cohomology class $\{a, b\} \in H^2(G, K^\times)$ from (10). Since only σ and $\sigma\tau$ move $\sqrt{a} \mapsto -\sqrt{a}$,

$$\begin{array}{llll} g_{\iota,\iota} = 1 & g_{\sigma,\iota} = 1 & g_{\tau,\iota} = 1 & g_{\sigma\tau,\iota} = 1 \\ g_{\iota,\sigma} = 1 & g_{\sigma,\sigma} = b & g_{\tau,\sigma} = 1 & g_{\sigma\tau,\sigma} = b \\ g_{\iota,\tau} = 1 & g_{\sigma,\tau} = 1 & g_{\tau,\tau} = 1 & g_{\sigma\tau,\tau} = 1 \\ g_{\iota,\sigma\tau} = 1 & g_{\sigma,\sigma\tau} = b & g_{\tau,\sigma\tau} = 1 & g_{\sigma\tau,\sigma\tau} = b. \end{array}$$

We now check that (a, b) and $\{a, b\}$ represent the same class in $H^2(G, K^\times)$, as promised by Proposition 2.1. The elements of $H^2(G, K^\times)$ are equivalence classes of factor sets under the relation (†) from above so we should be able to find some collection $\{u_\sigma \in K^\times : \sigma \in G\}$ such that

$$g_{\sigma,\tau} = \frac{u_\sigma \sigma(u_\tau)}{u_{\sigma\tau}} f_{\sigma,\tau}$$

holds for all $f_{\sigma,\tau}$ and $g_{\sigma,\tau}$. In fact, (†) holds using the function

$$u_\iota = 1, \quad u_\sigma = \sqrt{b}, \quad u_\tau = -1, \quad u_{\sigma\tau} = \sqrt{b}.$$

Computing the class $[a_{\sigma,\tau}] \in H^2(G, K^\times)$ using (14) gives

$$[a_{\sigma,\tau}] = (a,b)(a,a)(b,b) = (a,ab)(b,b) = (a,ab)(b,-1),$$

the simplification following as in the proof Proposition 2.1. We compute the class using equation (16). By definition, the Hasse invariants for Q_1 and Q_2 are the values $\epsilon(Q_1) = (a,a)(a,b)(b,b)$ and $\epsilon(Q_2) = (1,1)$ so

$$[a_{\sigma,\tau}] = (1,ab)(1,1)(a,a)(a,b)(b,b) = (1,ab)(a,ab)(b,-1) = (a,ab)(b,-1)$$

which is equal to that above.

The Clifford algebra $C(V,Q_1)$ is isomorphic to the quaternion algebra $A = \left(\frac{a,b}{\mathbb{Q}}\right)$ with the relations $\alpha^2 = a, \beta^2 = b, \alpha\beta = -\beta\alpha$. The class of A in $Br(K/\mathbb{Q})$ corresponds to the class of $\{a,b\}$ via Theorem 4.10. The field $E = \mathbb{Q}(\alpha)$ is a maximal subfield of A. Let H=Gal$(E/\mathbb{Q}) = \{\iota, \sigma\}$ where $\sigma(\alpha) \mapsto -\alpha$. An element $s_\sigma \in A^\times$ such that $s_\sigma \alpha s_\sigma^{-1} = -\alpha$ is given by $s_\sigma = \beta$. Set $s_\iota = 1 \in A^\times$. Then the set $\{s_\iota, s_\sigma\}$ is a basis for A as an E-vector space: $A = Es_\iota \oplus Es_\sigma$. Take $\{1, \alpha\}$ as a basis for $E/\mathbb{Q}$. As in Proposition 4.8, the set $\{1 \cdot s_\iota, 1 \cdot s_\sigma, \alpha \cdot s_\iota, \alpha \cdot s_\sigma\}$ is a basis for A as a $\mathbb{Q}$-vector space. Indeed, this is none other than the basis $\{1, \beta, \alpha, \alpha\beta\}$. Recall that $K = \mathbb{Q}(\sqrt{a}, \sqrt{b})$, and Gal$(K/\mathbb{Q}) = \{\iota, \sigma, \tau, \sigma\tau\}$ with $K^\tau = E$.

The restriction $\varphi\colon$ Gal$(K/\mathbb{Q}) \to$ Gal$(E/\mathbb{Q})$ is given by

$$\varphi\colon \sigma \mapsto \sigma, \quad \varphi\colon \tau \mapsto \iota.$$

The computation of the factor set of A relative to E, $\{a_{\sigma,\tau} \in E^\times \colon \sigma, \tau \in H\}$ yields the elements

$$a_{\iota,\iota} = a_{\iota,\sigma} = a_{\sigma,\iota} = 1, \quad a_{\sigma,\sigma} = b.$$

Given the factor set $\{a, b\} \in H^2(\mathrm{Gal}(K/\mathbb{Q}), K^\times)$ computed above that was defined by $\{g_{\sigma,\tau} \in K^\times \colon \sigma, \tau \in \ \mathrm{Gal}(K/\mathbb{Q})\}$, we have inflation $\varphi^* : H^2(H, E^\times) \to H^2(G, K^\times)$ defined by $\varphi^*\big([a_{\sigma,\tau}]\big) = \{a, b\}$ with

$$\varphi^*\big([a_{\sigma,\tau}]\big) \doteq [a_{\varphi(\sigma),\varphi(\tau)}].$$

Then $a_{\varphi(\sigma),\varphi(\tau)} = g_{\sigma,\tau}$ for all $\sigma, \tau \in G$ as desired.

Bibliography

[1] David S. Dummit and Richard M. Foote. *Abstract algebra*. John Wiley & Sons Inc., Hoboken, NJ, third edition, 2004.

[2] Benson Farb and R. Keith Dennis. *Noncommutative algebra*, volume 144 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1993.

[3] Max-Albert Knus. *Quadratic forms, Clifford algebras and spinors*, volume 1 of *Seminários de Matemática [Seminars in Mathematics]*. Universidade Estadual de Campinas, Instituto de Matemática, Estatística e Ciência da Computação, Campinas, 1988.

[4] James S Milne. Algebraic groups and arithmetic groups (v1.01), 2006. Available at www.jmilne.org/math/.

[5] J.S. Milne. Class field theory (v4.00), 2008. Available at www.jmilne.org/math/.

[6] J.-P. Serre. *A course in arithmetic*. Springer-Verlag, New York, 1973. Translated from the French, Graduate Texts in Mathematics, No. 7.

[7] Jean-Pierre Serre. *Galois cohomology*. Springer-Verlag, Berlin, 1997. Translated from the French by Patrick Ion and revised by the author.

[8] T. A. Springer. On the equivalence of quadratic forms. *Nederl. Akad. Wetensch. Proc. Ser. A 62 = Indag. Math.*, 21:241–253, 1959.

[9] John Tate. Galois cohomology. In *Arithmetic algebraic geometry (Park City, UT, 1999)*, volume 9 of *IAS/Park City Math. Ser.*, pages 465–479. Amer. Math. Soc., Providence, RI, 2001.